

イタルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、

アプリケーション層フィルタリングのためのフィルタパラメータを含む請求項1に記載のシステム。

6. 上記セキュリティ機能は、認証プロトコルを含む請求項1に記載のシステム。

7. 上記セキュリティ機能は、オーデットを含む請求項1に記載のシステム。

8. 上記セキュリティ機能は、許可を含む請求項1に記載のシステム。

9. 上記ノードセットは、中継器の機能を実行するノードを含み、そして上記セキュリティ機能は、中継器の機能に媒体アクセス制御MAC層フィルタリングを含む請求項1に記載のシステム。

10. 上記ノードセットは、データリンク層スイッチの機能を実行するノードを含み、そして上記セキュリティ機能は、スイッチ機能に媒体アクセス制御MAC層フィルタリングを含む請求項1に記載のシステム。

11. 上記ノードセットは、ネットワーク層ルータ指定機能を実行するノードを含み、そして上記セキュリティ機能は、ルータ指定機能にネットワーク層フィルタリングを含む請求項1に記載のシステム。

12. 上記ノードセットは、多数のプロトコル層ルータ指定機能を実行するノードを含み、そして上記セキュリティ機能は、認証機能を含む請求項1に記載のシステム。

13. 上記ノードセットは、ネットワーク層ルータ指定機能を実行するノード及びデータリンク層スイッチ機能を実行するノードを含み、そして上記セキュリティ機能は、媒体アクセス制御MAC層フィルタリング及びネットワーク層フィルタリングを含む請求項1に記載のシステム。

14. 上記ノードセットは、多数のプロトコル層ルータ指定機能を実行するノードを含み、そして上記セキュリティ機能は、認証を含む請求項13に記載のシステム。

15. 上記トポロジーデータ記憶装置は、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータを含む請求項1に記載

のシステム。

16. 上記トポロジーデータ記憶装置は、ノードセットの外部のノードへ至る

ネットワークリンクに接続されたノードと、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含み、そして

上記セキュリティポリシーステートメントは、能動的ノードと、受動的ノードと、ノードセットの外部のノードへ至るネットワークリンクに進行する通信とに対してセキュリティポリシーを指示する請求項1に記載のシステム。

17. 上記コンフィギュレーションインターフェイスは、スク립ト言語を解読してセキュリティポリシーステートメントを決定するスク립トインタープリターを含む請求項1に記載のシステム。

18. 上記トポロジーデータ記憶装置は、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含む請求項1に記載のシステム。

19. 上記セキュリティポリシーステートメントは、1つ以上の最終ステーションのソースセットと、1つ以上の最終ステーションの行先セットとの間の通信に対するセキュリティポリシーを指示する請求項18に記載のシステム。

20. 上記コンフィギュレーションドライバは、受動的ノードにリンクされた能動的ノードに対してコンフィギュレーションデータを発生することにより受動的ノードのセキュリティポリシーを実施するリソースを含む請求項18に記載のシステム。

21. 上記スク립ト言語は、ソースセット識別子、行先セット識別子、通信アクティビティ識別子、及び識別されたソースセットと識別された行先セットとの間の識別された通信アクティビティに対するルールを含むセキュリティポリシーステートメントを指定するシンタックスを含む請求項17に記載のシステム。

22. 上記シンタックスは、更に、ルールを実施すべき位置の識別子を含む請求項21に記載のシステム。

23. 上記コンフィギュレーションドライバは、トポロジーデータ記憶装置

のデータに基づいて実施できないセキュリティポリシーテストメントを識別するためのリソースを含む請求項21に記載のシステム。

24. ノードセットの特定ノードと通信する永続的記憶能力を有するコンフィ

ギュレーション記憶装置を備え、そして上記コンフィギュレーションドライバは、特定ノードに対するコンフィギュレーションデータをコンフィギュレーション記憶装置に送信する請求項1に記載のシステム。

25. 上記コンフィギュレーション記憶装置は、通信リンクによって特定ノードに接続される請求項24に記載のシステム。

26. 上記トポロジータータ記憶装置は、ネットワーク層アドレス、媒体アクセス制御MAC層アドレス、ユーザ識別子、特定ノードがセキュリティポリシーを実施する信頼性があるかどうか、実施できるセキュリティポリシーの形式、及び他のノードへのその接続を含む特定ノードの情報を与えるデータ構造体を備えている請求項1に記載のシステム。

27. 上記セキュリティポリシーテストメントは、ネットワークの1つ以上の最終ステーションを含むソースセットと、ネットワークの1つ以上の最終ステーションを含む行先セットとの間の通信に対するセキュリティポリシーを指示し、そして上記コンフィギュレーションドライバは、ネットワークのノードセット内の指示されたセキュリティポリシーを実施することのできるカット頂点セットのノードを識別し、そしてカット頂点セットのノードにコンフィギュレーションデータを確立するためのリソースを含む請求項1に記載のシステム。

28. 上記カット頂点セットは、最小のカット頂点セットより成る請求項27に記載のシステム。

29. 複数の形式のノードを含むネットワークにセキュリティを与えるシステムであって、ネットワーク内のノードセットのノードは、対応するノード形式に適合したコンフィギュレーションデータにตอบสนองして実行されるセキュリティ機能を含むようなシステムにおいて、

ネットワーク内のノードセットのセキュリティ機能と、ノードセット内のノードの相互接続に関する情報を記憶するトポロジータータ記憶装置であって、1

つ以上のプロトコル層におけるアドレス、特定ノードがセキュリティポリシーを実施する信頼性があるかどうか、特定ノードが実施できるセキュリティポリシーの形式、及び特定ノードと他のノードとの接続を含む特定ノードの情報を与えるデータ構造体を有するトポロジータータ記憶装置と、

上記トポロジータータ記憶装置に接続されたコンフィギュレーションインターフェイスであって、このインターフェイスは、ネットワークにおける1つ以上の終端ステーションのソースセットと1つ以上の終端ステーションの行先セットとの間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーテストメントを受け取る入力と、スクリプト言語を解読してセキュリティポリシーテストメントを決定するためのスクリプトインタプリタとを含み、上記スクリプト言語は、ソースセット識別子、行先セット識別子、通信アクティビティ識別子、及び識別されたソースセットと識別された行先セットとの間の識別された通信アクティビティに対するルールを含むセキュリティポリシーテストメントを指定するシンタックスを含むようなコンフィギュレーションインターフェイスと、

上記ネットワーク、コンフィギュレーションインターフェイス及びトポロジータータ記憶装置に接続され、セキュリティポリシーテストメントを、ネットワーク内の種々の形式のノードに対するコンフィギュレーションデータに変換し、そしてそのコンフィギュレーションデータをノードへと搬送するリソースを含むコンフィギュレーションドライバと、
を備えたことを特徴とするシステム。

30. 上記ノードセットは、フィルタパラメータに基づいて媒体アクセス制御MAC層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、MAC層フィルタリングのためのフィルタパラメータを含む請求項29に記載のシステム。

31. 上記ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ネットワーク層フィルタリングのためのフィルタパラメータを含む請求項29に

記載のシステム。

32. 上記ノードセットは、フィルタリングパラメータに基づいて搬送層フィラタリングを与えるノードを含み、そしてコンフィギュレーションデータは、搬送層フィルタリングのためのフィルタパラメータを含む請求項29に記載のシステム。

33. 上記ノードセットは、フィルタパラメータに基づきアプリケーション層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、アプリケーション層フィルタリングのためのフィルタパラメータを含む請求項29に記載のシステム。

34. 上記トポロジデータ記憶装置は、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含む請求項29に記載のシステム。

35. 上記トポロジデータ記憶装置は、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータを含む請求項29に記載のシステム。

36. 上記セキュリティポリシーステートメントは、ノードセットの外部のノードへ至るネットワークリンクに進行する通信に対するセキュリティポリシーを指示する請求項35に記載のシステム。

37. 上記シンタックスは、更に、ルールを実施すべき位置の識別子を含む請求項29に記載のシステム。

38. 上記コンフィギュレーションドライバは、トポロジデータ記憶装置のデータに基づいて実施できないセキュリティポリシーステートメントを識別するためのリソースを備えている請求項29に記載のシステム。

39. ノードセットの特定ノードと通信する永続的記憶能力を有するコンフィギュレーション記憶装置を備え、そして上記コンフィギュレーションドライバは、特定ノードに対するコンフィギュレーションデータをコンフィギュレーション記憶装置に送信する請求項29に記載のシステム。

40. 上記コンフィギュレーション記憶装置は、通信リンクにより特定のノード

ドに接続される請求項39に記載のシステム。

41. 上記コンフィギュレーションドライバは、指示されたセキュリティポリシーを実施することのできるカット頂点セットのノードを識別しそしてカット頂点セットのノードにコンフィギュレーションデータを確立するためのリソースを含む請求項29に記載のシステム。

42. 上記カット頂点セットは、最小のカット頂点セットより成る請求項41

に記載のシステム。

43. 複数の形式のノードのセットを含むネットワークにファイアウォールシステムを確立する方法であって、ネットワーク内の上記ノードセットのノードは、対応するノードに適応したコンフィギュレーションデータに応答して実行されるセキュリティ機能を含み、上記方法は、

上記ノードセットのノードにおいて働くセキュリティ機能と、上記ノードセットのノードの相互接続とに関する情報を含むトポロジデータを与え、

上記ノードセットの最終システム間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを与え、

上記トポロジデータにตอบสนองして、セキュリティポリシーステートメントを、ノードセットのノードにおいて働くセキュリティ機能に対するコンフィギュレーションデータへと変換し、そして

ネットワーク内のノードにおいてセキュリティ機能にコンフィギュレーションデータを確立する、

という段階を備えたことを特徴とする方法。

44. 上記トポロジデータは、1つ以上のプロトコル層のアドレス、特定ノードがセキュリティポリシーを実施する信頼があるかどうか、特定ノードが実施できるセキュリティポリシーの形式、及び特定ノードと他のノードとの接続を含む特定ノードの情報を与えるデータ構造体を備えている請求項43に記載の方法。

45. セキュリティポリシーステートメントを与える上記段階は、スクリプト言語を解釈して、セキュリティポリシーステートメントを決定することを含み、

上記スク립ト言語は、ソース識別子、行先識別子、通信アクティビティ識別子、及び識別されたソースと識別された行先との間の識別された通信アクティビティに対するルールを含むセキュリティポリシーステートメントを指定するためのシンタックスを含む請求項43に記載の方法。

46. 上記シンタックスは、更に、ルールを実施すべき位置の識別子を含む請求項45に記載の方法。

47. 上記確立段階は、ノードと通信する永続的な記憶装置にネットワークのコンフィギュレーションデータを送信することを含む請求項43に記載の方法。

48. 少なくとも1つのノードに対し、ノードと通信する永続的な記憶装置は、ノードにとってローカルであり、そして少なくとも1つの他のノードに対し、ノードと通信する永続的な記憶装置は、ノードから離れている請求項47に記載の方法。

49. 少なくとも1つのノードに対し、ノードと通信する永続的な記憶装置は、ノードから離れており、ノードにコンフィギュレーションデータを確立する上記段階は、永続的な記憶装置にコンフィギュレーションデータを送信した後に、コンフィギュレーションデータが変化したことをノードのセキュリティ機能に通知することを含む請求項47に記載の方法。

50. 上記トポロジーデータは、セキュリティポリシーを実施できる能動的ノードと、セキュリティポリシーを実施できないか又は実施する信頼性のない受動的ノードとを指示するデータを含む請求項43に記載の方法。

51. 上記トポロジーデータは、ノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータを含む請求項50に記載の方法。

52. 上記セキュリティポリシーステートメントは、ノードセットの外部のノードへ至るネットワークリンクに進行する通信に対してセキュリティポリシーを指示する請求項51に記載の方法。

53. 上記変換段階は、受動的ノードのセキュリティポリシーを実施するために、受動的ノードにリンクされた能動的ノードのコンフィギュレーションデータ

を発生することを含む請求項50に記載の方法。

54. 上記変換段階は、トポロジーデータ記憶装置のデータに基づいて実施できないセキュリティポリシーステートメントを識別することを含む請求項43に記載の方法。

55. 上記ノードセットは、フィルタパラメータに基づいてMAC層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、MAC層フィルタリングのためのフィルタパラメータを含む請求項43に記載の方法。

56. 上記ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、ネットワーク層フィルタリングのためのフィルタパラメータを含む請求項43に記載の方法。

記載の方法。

57. 上記ノードセットは、フィルタパラメータに基づいて搬送層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、搬送層フィルタリングのためのフィルタパラメータを含む請求項43に記載の方法。

58. 上記ノードセットは、フィルタパラメータに基づきアプリケーション層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、アプリケーション層フィルタリングのためのフィルタパラメータを含む請求項43に記載の方法。

59. 上記セキュリティ機能は、許可を含む請求項43に記載の方法。

60. 上記セキュリティ機能は、認証を含む請求項43に記載の方法。

61. 上記セキュリティ機能は、オーデットを含む請求項43に記載の方法。

62. 上記ノードセットは、インターネットワークプロトコルIPフィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、IPフィルタパラメータを含む請求項43に記載の方法。

63. 上記ノードセットは、インターネットワークプロトコル及び搬送制御プロトコルTCP/IPフィルタパラメータに基づいてフィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、TCP/IPフィルタパラメータ

タを含む請求項43に記載の方法。

64. 複数の形式のノードのセットを含むネットワークにファイアウォールシステムを確立する方法であって、ネットワーク内の上記ノードセットのノードは、対応するノードに適応したコンフィギュレーションデータにตอบสนองして実行されるセキュリティ機能を含み、上記方法は、

上記ノードセットのノードにおいて動くセキュリティ機能と、上記ノードセットのノードの相互接続とに関する情報を含むトポロジーデータを与え、
上記ノードセットにおける最終ステーションのソースセットと最終ステーションの行先セットとの間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを与え、
トポロジーデータ及びセキュリティポリシーステートメントにตอบสนองして、セキ

ュリティポリシーステートメントを実施できるノードより成るカット頂点セットのノードを識別し、これは、ネットワークから除去された場合に、ソースセットを行先セットから分離するものであり、
識別されたカット頂点セット及びセキュリティポリシーステートメントにตอบสนองして、カット頂点セットのノードにおいて動くセキュリティ機能に対するコンフィギュレーションデータへと変換し、そして

カット頂点セットのノードにおいてセキュリティ機能にコンフィギュレーションデータを確立する、
という段階を備えたことを特徴とする方法。

65. 上記トポロジーデータは、アドレス、特定ノードがセキュリティポリシーを実施する信頼があるかどうか、特定ノードが実施できるセキュリティポリシーの形式、及び特定ノードと他のノードとの接続を含む特定ノードの情報を与えるデータ構造体を備えている請求項64に記載の方法。

66. セキュリティポリシーステートメントを与える上記段階は、スク립ト言語を解読して、セキュリティポリシーステートメントを決定することを含み、上記スク립ト言語は、ソース識別子、行先識別子、通信アクティビティ識別子、及び識別されたソースと識別された行先との間の識別された通信アクティビテ

ィに対するルールを含むセキュリティポリシーステートメントを指定するためのシンタックスを含む請求項64に記載の方法。

67. 上記確立段階は、カット頂点セットのノードと通信する永続的な記憶装置にネットワークのコンフィギュレーションデータを送信することを含む請求項64に記載の方法。

68. 少なくとも1つのノードに対し、ノードと通信する永続的な記憶装置は、ノードにとってローカルであり、そして少なくとも1つの他のノードに対し、ノードと通信する永続的な記憶装置は、ノードから離れている請求項67に記載の方法。

69. 上記ノードセットは、インターネットワークプロトコルIPフィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、IPフィルタパラメータを含む請求項64に記載の方法。

70. 上記ノードセットは、インターネットワークプロトコル及び搬送制御プロトコルTCP/IPフィルタパラメータに基づいてフィルタリングを与えるノードを含み、そしてコンフィギュレーションデータは、TCP/IPフィルタパラメータを含む請求項64に記載の方法。

71. 上記カット頂点セットは、最小のカット頂点セットより成る請求項64に記載の方法。

【発明の詳細な説明】

多層型ファイアウォールシステム

発明の分野

本発明は、ネットワークのセキュリティ機能を確立して実施することに保り、より詳細には、複数のプロトコル層にセキュリティ機能を確立してネットワークに多層型ファイアウォールを確立するシステムに係る。

先行技術の説明

セキュリティは、いわゆるイントラネットを操作する企業内部と、世界的規模のグローバルデータネットワークとの両面で、ネットワークユーザにとって益々重要なものとなってきている。ネットワークのセキュリティを確保する目的で、新しい技術が開発されている。開発されたセキュリティの特徴は、少なくとも、次の製品分類を含む。(1) フィルタリング、(2) アクセス制御、(3) 保護通信、(4) セキュリティ支援、及び(5) セキュリティポリシー管理。

フィルタリングは、パケット又はフレームをそれらのヘッダ又はデータ内の値に基づいてドロップし又は変換することを含む。アクセス制御は、ユーザ又はユーザが開始した通信に、特定の計算リソースへのアクセスを与えねばならないかどうか判断することを含む。保護通信は、制御情報又はデータが変更もされないし無許可の個人によって読み取られもしないよう確保するプロセスを指す。セキュリティ支援製品形式は、ネットワークデバイスにおいてシステムの他の部分のセキュリティを確保するための支援を与える。セキュリティポリシー管理は、ネットワークにおいてセキュリティのポリシーを定義するデータを管理することを指す。

このような種類のセキュリティ特徴は、現在のシステムでは、特定のネットワークデバイスにおいて実施される。セキュリティが実施されるネットワークデバイスは、通常のターミナルや最終システムに加えて、次のようなデバイスを含む。(1) ネットワークインターフェイスカード(NIC)及びモデム、(2) 中継器、(3) スイッチ、(4) ルータ、(5) ラインサーバ、パケットサーバ及びアクセスサーバを含むリモートアクセス装置、及び(6) ネットワークマネージャメントシステム。特定の製品ファミリにセキュリティを確立するための製品

は存

在するが、ネットワークに見られる種々の全ての装置分類において製品の利点を採り入れられるシステムは、膨大な管理を必要とする。種々様々なネットワーク中間装置及びターミナルを伴うネットワークにおいては、全ての種々のプロトコルレベル及び全ての種々のシステムにおいてセキュリティポリシーの確立を管理するためのアドミニストレータが必要とされる。

例えば、ある公知システムでは、仮想ローカルエリアネットワーク(VLAN)と称する構成を確立することができる。VLANを構成することにより、グループのメンバーシップが制御される。例えば、ポート番号、媒体アクセス制御アドレス、層3プロトコル形式、層3アドレス、及び層3パケットのバターンに一致するユーザ定義基準を使用して、このような装置におけるVLANメンバーシップを定義することができる。同様のバターンマッチングは、例えば、層3ないし7のプロトコルデータを含んでもよい。他のシステムは、リモートアクセスシステムにおいてコールごとのフィルタリングをサポートする。これは、顧客が色々な種類のトラフィックをユーザごとに許可又は拒絶できるようにする。種々様々な他のセキュリティシステムも市場で入手できる。

しかしながら、種々のセキュリティ特徴、種々のデバイス、及びそれらが動作するプロトコルレベルは、セキュリティ特徴の利用者にとって著しい管理の問題を引き起こす。複雑であるために、ネットワークの全ての層及びデバイス形式にわたって整合したセキュリティポリシーを確立することは困難であると共に、これが首尾良く実施されたとしてもこのようなシステムを維持することは特に困難である。

更に、ネットワークの進歩に伴い、特定のセキュリティ機能に参加することのできない遺産的システムとしばしば称される古い装置が残される。それ故、ネットワークに追加されるセキュリティ機能は、ネットワーク全体に首尾良く浸透できないことがある。或いは又、ネットワークにおける遺産的システムの存在が、セキュリティシステムの整合及び実施を更に複雑なものにする。

従来、専用ネットワークを外部からの侵入に対して保護するルータ及びアプ

ケーションプロキシゲートウェイのような境界装置としてファイアウォールが実施されている。しかしながら、おそらく、企業損失の50%ないし80%は

内部の者の侵入、例えば、不満を抱えた又は機会に恵まれた従業員によるものである。従って、会社のイントラネットに関するほとんどのセキュリティ要求は、内部侵入に対する保護である。

更に、現代企業の経営は、その経済性から、会社にとって外注先での作業や他の会社との共同運営が益々必要になっている。現代企業では情報技術が業務の実施に日に日に浸透してきているので、このような外注作業や共同運営は、会社が電子的手段を用いて互いに情報を共用することを必須とする。この情報が、会社の情報財産の他部分を保持するものから分離された装置において入手できることは稀である。従って、外注作業や共同運営には、会社にとってそのイントラネットの一部分へ別の会社がアクセスするのを許可することが必要となる。更に、各々の外注作業や共同運営の構成は、通常、会社の異なる部門や子会社を伴う。これは、少なくとも1つの外部関係者によりアクセスできる会社の情報財産の割合が著しく大きくなることを意味する。

従来の境界ファイアウォールは、2つの事柄、即ち内部の者による脅迫や、広く分散したデータの外部共用によって生じるセキュリティ要件を満足するのにほとんど適していない。境界ファイアウォールは、内部の者による脅迫に対処するのには全く不適である。それらは、外部の侵入者が会社のイントラネットに侵入するのを排除することを意味するが、内部の者がそれを行うのを阻止することはできない。

会社の情報への外部アクセスを受け入れるためには、必要な情報を流せるように境界ファイアウォールに「ホール」を形成しなければならない。極端な場合には、各部門は、会社のファイアウォールを全く簡単にバイパスして、外注先や共同経営の会社、又はその社員へ直接接続することができる。

これらの要件を満足する1つの解決策は、会社のイントラネットを多数の部分に分割し、そしてそれらの間に境界ファイアウォールを配置することである。こ

の解決策は、価値があるが、会社のイントラネットにポトルネックが生じることになる。即ち、内部のファイアウォールが会社内の業務遂行に悪影響を及ぼす。区画化がより細かくなるとつれて、ファイアウォール区画の外部のリソースへのアクセスは、その遂行性が益々悪くなる。

この問題に対する別の解決策は、ファイアウォールの機能をプロトコルハイアラキーの下位層へと分散することである。従って、例えば、ネットワークインターフェイスカード、中継器及びスイッチが、あるファイアウォールパケットフィルタリング作業を行う場合には、従来パケットフィルタリングを行っていたルータにおいて相当の処理が軽減され、それ故、所与のコストに対して良好な性能を発揮することができる。更に、ファイアウォールの分散化は、規模縮減の良好な機会を与える。即ち、ネットワークが成長するにつれて、フィルタリングを実行するのに使用できるリソースも当然成長する。これは、例えば、内部の境界ファイアウォールにおいて生じることのあるチョークポイントの発生を防止する。

通常、公知技術では、パケットフィルタリングのようなファイアウォール機能は、単一のノード、又は同じファイアウォールルールを伴う同様のノードのグループに設けられる。これらのノードは、ネットワークの外部からの侵入に対してネットワークを保護するためにネットワークの境界に展開される傾向にある。しかしながら、この解決策は、ネットワークの拡張につれて充分に規模を広げることができない。更に、ネットワークセキュリティに対して制御の粒度が非常に粗くなる。実施することのできる種々の異なる解決策は、個々のシステムがネットワーク内でいかに相互作用するかを理解することが困難である。更に、これらの個々のシステムは、ネットワーク内部の無許可の行為から保護するために適用したときには、通常、著しい性能上の問題を引き起こす。(例えば、「インターネットファイアウォールの構築(Building Internet Firewalls)」、チャプマン氏等著、オレレイリ&アソシエーツ、1995年9月;「インターネットファイアウォール及びセキュリティ(Internet Firewall and Security)」、3コム・テクニカルレポート、1996年、セメリア著を参照されたい)。

従って、ネットワークシステムの多数の層にわたり整合されたセキュリティポ

リシーを実行することのできるシステムの実施が要望される。

発明の要旨

本発明は、多数のプロトコル層で動作しそしてセキュリティ機能を有するノードを備えたネットワークにおいてセキュリティを与えるシステムを提供する。ルータ、リモートアクセス装置、スイッチ、中継器及びネットワークカードのよう多数のネットワークデバイス、並びにセキュリティ機能を有する最終システムプロセスは、ネットワークにおける分散型ファイアウォール機能の実施に貢献するように構成される。ネットワークのファイアウォール機能を種々のネットワークデバイス及び最終システムに分散することにより、浸透したファイアウォールが実施される。浸透した多層型ファイアウォールは、ファイアウォールがいかに振舞わねばならないかを定義するポリシーデータを受け入れるポリシー定義要素を含む。このポリシー定義要素は、集中化された要素であってもよいし、又はネットワークにわたって分散された要素でもよい。又、多層型ファイアウォールは、定義されたポリシーを実施するのに使用されるネットワークデバイスの集合も、多数のプロトコル層にわたりネットワークデバイスのこの集合において動作するセキュリティ機能は、特定のデバイスが、ネットワークの当該部分に関するポリシーの部分を実施するように、ポリシー定義要素により整合される。

例えば、ネットワークのルータは、トラフィックがルータを横切るところのシステム及びネットワークデバイスに関与するポリシーの部分を実施する。スイッチは、トラフィックがスイッチを横切るところのシステム及びネットワークデバイスに関与するポリシーの部分を実施する。中継器は、トラフィックが中継器を横切るところのシステム及びネットワークデバイスに関与するポリシーの部分を実施する。ネットワークインターフェースカードは、それが接続されたシステム又はデバイスに関与するポリシーの部分を実施する。更に、多層型ファイアウォールにはネットワークの他の部分が含まれ、例えば、最終システムのオペレーティングシステム及びアプリケーションや、ネットワークトラフィックを制御しそしてネットワークトラフィックを監視するリモートアクセス装置のネットワークマネージメントシステムや、他の補助的なシステム、例えば、本発明の浸透した

多層型ファイアウォールが実施されるネットワークデバイスの集合に含まれるノードサーバ及びファイナルサーバが含まれる。

本発明は、多数のネットワークデバイス及び最終システムにおいて整合されたアクセス制御、協働保護通信特徴、及び全体的なセキュリティポリシー管理を与える。セキュリティアドミニストラータには、ネットワークのセキュリティ特性を監視できるようにする便利で且つ明確な制御システムが設けられる。更に、本

発明は、セキュリティサービスにおける不必要な冗長性を減少できるようにし、遺産的システムサポートのエリアにおいて著しい顧客の要求を満足し、コスト効率を与え、そして複雑さを低減させる。

従って、本発明は、1つの観点によれば、ノードを含むネットワークにセキュリティを与えるシステムを特徴とすることができ、ネットワークのノードセットにおけるノードは、1つ又は多数のプロトコル層で動作するセキュリティ機能を含み、そしてノードの各形式に適応されたフォーマットを有する構成データに応答してこのようなセキュリティ機能を実行する。システムは、ネットワークのノードセットにおいて動作するセキュリティ機能に関する情報及びネットワークにおけるノードの相互接続に関する情報を記憶するトポロジーデータ記憶装置を備えている。このトポロジーデータ記憶装置にはコンフィギュレーションインタフェースが接続される。このインタフェースは、ネットワークのノード間で実施されるべきセキュリティポリシーを指示するセキュリティポリシーステートメントを受け取るための入力を含む。ネットワーク、コンフィギュレーションインターフェース及びトポロジーデータ記憶装置にはコンフィギュレーションドライバが接続される。このコンフィギュレーションドライバは、セキュリティポリシーステートメントを、ネットワークのノードに必要なフォーマットのコンフィギュレーションデータへと変換するリソースであって、各ノードに対して使用できる通信チャネルを用いてコンフィギュレーションデータをノードへ送信するリソースを含む。

本発明の種々の観点によれば、ノードは、媒体アクセス制御MAC層を含む多数のプロトコル層を実行し、そしてノードセットは、フィルタパラメータに基づ

いてMAC層のフィルタリングを与えるノードを含む。コンフィギュレーションデータは、MAC層のフィルタリングに対するフィルタパラメータを含む。別の観点において、多数のプロトコル層は、インターネットプロトコルIP層のようなネットワーク層を含む。この観点によれば、ノードセットは、フィルタパラメータに基づいてネットワーク層フィルタリングを与えるノードを含む。コンフィギュレーションデータは、このようなノードにおけるネットワーク層フィルタリングのためのフィルタパラメータを含む。別の観点によれば、多数のプロトコル

層は、インターネットプロトコルを介して動作する搬送制御プロトコルTCPのような搬送層機能を含む。この観点によれば、コンフィギュレーションドライバースは、セキュリティポリシーステートメントを、フィルタリングのような搬送層機能、フィルタリングのようなアプリケーション層機能及び/又はプロトコルスタックの上位層における機能に対するコンフィギュレーションデータに変換するリソースを含む。このような上位層機能は、例えば、認証プロトコル、許可プロトコル、オーデッドプロトコル及び他のセキュリティ機能を含む。フィルタリング、アクセス制御、保護通信及びセキュリティ支援特徴を実行する種々のデバイスは、ネットワークインフラストラクチャにおいて分散され、そして本発明により整合形態で管理される。

本発明の他の観点によれば、コンフィギュレーションインターフェイスは、セキュリティポリシーステートメントを決定するためにスク립ト言語を解釈するスク립トインタープリターを含む。スク립ト言語は、キーボード又はグラフィックユーザインターフェイスによって入力することができる。スク립ト言語のサポートにおいて、トポロジーデータ記憶装置は、セキュリティポリシーを実施することのできるネットワーク内の能動的ノードと、セキュリティポリシーを実施できないか又はそれを実施する信頼のない受動的ノードとを指示するデータを含む。更に、トポロジーデータ記憶装置は、セキュリティフレームワーク内のノードセットの外部のノードへ至るネットワークリンクに接続されたノードを指示するデータも含む。セキュリティポリシーステートメントは、最終システムのセキュリティポリシーを指示する。能動的ノード、受動的ノード、及びセキュリ

ティネットワークの外部のノードへ至るネットワークリンクに接続されたノードは、ポリシーを実行するように構成される。本発明の別の観点によれば、スク립ト言語は、ソースノード又はソースグループのためのソース識別子と、先行ノード又は先行グループのための先行識別子と、通信アクティビティ識別子と、識別されたソースと識別された先行との間の識別された通信アクティビティのためのルールとを含むセキュリティポリシーステートメントを特定するシンタックスを含む。本発明の1つの観点によれば、シンタックスは、更に、ルールを実施すべき位置（即ち、ソース、先行、ソース及び先行の両方、或いは中間ノード）の

識別子を含む。

本発明の更に別の観点によれば、セキュリティポリシーステートメントは、ネットワーク内の1つ以上の最終ステーションを含むソースセットと、ネットワーク内の1つ以上の最終ステーションを含む先行セットとの間で通信するためのセキュリティポリシーを指示する。コンフィギュレーションドライバースは、ネットワークのノードセット内の指示されたセキュリティポリシーを実施することのできるノードのカット頂点セットを識別すると共にそのカット頂点セット内のノードにおいてコンフィギュレーションデータを確立するためのリソースを含み、ここで、カット頂点セットは、ネットワークから除去された場合にソースセットを先行セットから分離する能動的ノードより成る。最適な実施形態においては、カット頂点セットは、最小のカット頂点セットより成る。

本発明の更に別の観点によれば、コンフィギュレーションドライバースは、受動的ノードにリンクされた能動的ノードに対してコンフィギュレーションデータを発生することにより受動的ノードのセキュリティポリシーを実施するためのリソースを含む。又、コンフィギュレーションドライバースのリソースは、トポロジー記憶装置のデータに基づいて実施できないセキュリティポリシーステートメントを識別する。

トポロジーデータ記憶装置は、1つの好ましい観点においては、セキュリティフレームワーク内に入るノードセット内の特定ノードに関する情報を与えるデータ構造体を含む。このデータ構造体は、ネットワーク層アドレス、MAC層アド

レス、上位層ユーザ識別子、搬送層のポート及びソケット番号、特定のノードがセキュリティポリシーを実施する信頼があるかどうか、ノードが実施できるセキュリティポリシーの形式、ポリシーを実施するのに使用される格差、セキュリティ構築に必要なコンフィギュレーションデータのフォーマット、及びノードとネットワーク内の他のノードとの接続のような情報を含む。

本発明の更に別の観点によれば、コンフィギュレーションドライバは、ネットワークに分散されたセキュリティ機能のためのコンフィギュレーションデータを発生する。コンフィギュレーションデータは、永続的な記憶能力を有するコンフィギュレーション記憶装置に記憶され、これは、コンフィギュレーションデータ

に関連したノードセットにおける特定のノードと通信する。ネットワーク内のあるデバイスのコンフィギュレーション記憶装置は、例えば、不揮発性のプログラムメモリ形態でデバイス自体に含まれる。別のシステムでは、コンフィギュレーション記憶装置は、ポリシーが実施されるノード以外のネットワーク内のノードに設けられ、そして通信リンクによってポリシーが実施される特定のノードに接続される。本発明のこの観点によれば、コンフィギュレーションドライバは、更新されたコンフィギュレーションデータをコンフィギュレーション記帳装置に送信し、その後、セキュリティ機能が実行されるノードに、記憶装置のコンフィギュレーションが更新されたことを通知する。このノードは、次いで、更新されたコンフィギュレーションデータを読み取り、そして更新されたポリシーの実行を開始する。

又、本発明は、より一般的には、ネットワークにファイアウォールシステムを確立する方法を特徴とすることができる。この方法は、ネットワーク内のノードにおいて動作するセキュリティ機能と、ネットワーク内のノードの相互接続とに関する情報を含むトポロジデータを与えることを含む。次いで、この方法は、当該ノードの形式（1つ又は複数）に合致するフォーマット及び通信チャネルを使用して、セキュリティ確保されたネットワーク内の最終システム間で実施されるべきセキュリティポリシーを含むセキュリティポリシーステートメントを与えることを含む。次いで、この方法は、トポロジデータにตอบสนองして、セキュリ

ティポリシーステートメントを、ネットワーク内で動作するセキュリティ機能のためのコンフィギュレーションデータに変換することを含む。最終的に、この方法は、ノードの種々の形式に合致するフォーマット及び通信チャネルを使用して、ネットワーク内の能動的なノードにおいてセキュリティ機能のコンフィギュレーションデータを確立することを含む。セキュリティ機能が1つの別の形態で動作するところの多数のプロトコル層は、少なくとも2つのプロトコル層、例えば、データリンク層、ネットワーク層、搬送層、並びにそのアプリケーション又は等効物の少なくとも2つを含む。

従って、本発明は、ネットワークインターフェイスカード、スイッチ、ルータ及びリモートアクセスシステムに設けられたセキュリティ機能の利点を取り入れ

、
そしてファイアウォール機能をネットワーク内の種々のデバイスへと移動して、浸透した多層型ファイアウォールを形成する機会をシステムアドミニストレータに与える。セキュリティ特徴は、多数のデバイスに対して多数の層に分散し、そしてコヒーレントなセキュリティポリシーマネジメントインターフェイスを用いて管理することができ、このインターフェイスは、ネットワークのセキュリティ特性を介して便利で且つ明確な制御をセキュリティアドミニストレータに与える。分散された機能と、便利で且つ明確な制御は、分散型リモート監視d r M ONのようなシステム、又は単一目的機能に向けられた他の精巧なネットワークシステムに対してのみ現存するファイアウォールの利点を拡張できるようにする。

。 フィルタリングルール及び保護通信インフラストラクチャ情報セットのよう なセキュリティポリシーデータを含むネットワークデバイスの数が増加するにつ れて、コヒーレントで且つ整合されたデータ管理を与えることが益々重要となる。 本発明は、種々の多層ネットワークにおいてセキュリティポリシー実施データを 管理及び分散するためのコヒーレントな解決策を提供する。

本発明の他の特徴及び効果は、添付図面、その詳細な説明及び請求の範囲から 明らかとなるう。

図面の簡単な説明

図1は、本発明による多層型ファイアウォールシステムを含むネットワークを示す簡単な図である。

図2は、本発明の多層型ファイアウォールシステムに含まれる種々のネットワーク要素を示す図である。

図3は、本発明による多層型ファイアウォールを実施するプロセスを示すフローチャートである。

図4は、本発明による多層型ファイアウォール機能を実施するための別の技術を示すフローチャートである。

図5は、本発明の多層型ファイアウォールシステムによりネットワーク内のノードにコンフィギュレーションデータを確立するのに含まれる段階を示すフローチャートである。

図6及び7は、図2の変形であって、本発明による例示的なセキュリティフレームワークを強調して示した図である。

好ましい実施形態の詳細な説明

先ず、図1ないし5を参照して本発明を詳細に説明する。図1は、概観図である。

図1において、ネットワーク10は複数のノードを含む。ネットワーク内の少なくとも1つのノードは、ネットワークマネージャメントステーション11又は他のセキュリティポリササーバを含む。ネットワーク内の他のノードは、スイッチ12と、リモートアクセス装置13と、ルータ14と、ネットワークインターフェイスカード及びそれをサポートするドライバソフトウェアを含む最終ステーション15と、中継器16とを備えている。従って、ネットワーク10には種々のネットワークデバイスが含まれる。スイッチ12、リモートアクセス装置13、ルータ14、最終ステーションのネットワークインターフェイスカード15及び中継器16は、全て、セキュリティポリサマネージャメントエージェント22、23、24、25及び26を各々含む。これらセキュリティポリサマネージャメントエージェント22-26は、種々のプロトコル層においてセキュリティ機

能を実行する。エージェントが実施される特定のネットワークデバイスを横断するプロトコル層と、他の構造的特徴とに基づいて、セキュリティ機能に使用される構造は、デバイス形式ごとに変化する。

図1に示す実施形態では、ネットワークマネージャメントステーション11は、トポロジーデータ記憶装置30と、コンフィギュレーションインターフェイスの前端31と、コンフィギュレーションドライバを構成するセキュリティポリサマネージャメント後端32とを備えている。トポロジーデータ記憶装置30は、ネットワークのノードにおいて多数のプロトコル層で動作するセキュリティポリサマネージャメントエージェント22-26より実行されるセキュリティ機能に関する情報を記憶する。又、このトポロジーデータベースは、ネットワークにおけるノードの相互接続も指示する。

コンフィギュレーションインターフェイスの前端31は、トポロジーデータベース30に接続される。これは、セキュリティポリサステータメントを受け取るための入力を含み、例えば、セキュリティポリサ言語のスク립トを与え、

このスク립トをインタープリタ-34により解釈して、セキュリティポリサステータメントを形成する。セキュリティポリサマネージャメントの後端32は、コンフィギュレーションインターフェイスの前端31及びトポロジーデータベース30に接続され、セキュリティポリサステータメントをネットワーク内のノードのコンフィギュレーションデータへと変換するリソースを含む。セキュリティポリサマネージャメントの後端32は、セキュリティポリサステータメントを実施すべきネットワーク内のノードにおいてセキュリティポリサマネージャメントエージェント22-26へのコンフィギュレーションデータを確立するコンフィギュレーションドライバを構成する。

コンフィギュレーションインターフェイスの前端31は、1つの実施形態においては、セキュリティポリサ言語のスク립トをシステムに入力するところのテキスト入力デバイスを含む。別の実施形態では、コンフィギュレーションシステムインターフェイスの前端31は、ユーザがセキュリティポリサステータメントを特定するところのグラフィックユーザインターフェイスを含む。各々の解

決策において、セキュリティポリシーステートメントを、そのポリシーが実施されるネットワーク内のノードの適当なプロトコルレベル及びデバイス形式に対するコンフィギュレーションデータへと変換することのできるシンタックスを有するセキュリティポリシースキンプットが与えられる。

セキュリティポリシー言語及びセキュリティポリシー言語前部

セキュリティポリシー言語は、ネットワーク内のアクティビティに対する制約を特定するのに使用される。このようなアクティビティは、中継器、スイッチ、ルータ、リモートアクセス装置等のネットワークデバイスと、ネットワークの最終システムとの両方によって行なわれるアクティビティを含む。多層ファイアウォールは、特定の設備に達したセキュリティポリシー言語で実施できるが、1つの言語を以下に例示する。

各最終システム及び能動的ネットワークデバイスは、そのセキュリティポリシーマネージメントエージェントに関連した1つ以上のネットワークアドレスを有し、そして1つ以上の他のネットワークデバイスに接続される。この情報は、セキュリティポリシー言語前部によりシステムアドミニストラタとの対話を介して

て得られると共に、トポロジーデータベースから得られる。システムアドミニストラタとの対話は、ユーザインタフェイスを経で行なわれるか、或いはファイルや他の記憶リソース、例えば、ドメインネームシステム(DNS)、ネットワークインフォメーションサービス(NIS)又は他のベースの読み取りによって行なわれる。最終システムは、それらが常にトポロジーデータベースから形成されたグラフに放置されるという点でネットワークデバイスとは区別される。

「ノード」という一般的な表現は、最終システム又はネットワークデバイスのいずれかを指す。最終システム(akaホスト)は、ポリシーステートメントにおいて識別されるノードである。例えば、管理の目的でネットワークデバイスがアクセスされるときには特殊なケースが生じる。このケースでは、ネットワークデバイスが最終システムの役割を果たす。

ネットワークの最終システムは、グループに属してもよい。グループは、名前が付けられ、そしてそれらのメンバーシップは、システムアドミニストラタ等

によるか又はトポロジーデータベースで実施される別の形態においてセキュリティポリシー言語前部への入力で確立される。この場合も、この入力、ユーザインタフェイスの対話によるか、又はセキュリティポリシー言語前部がファイル又は他のデータベースを読み取ることにより得ることができる。最終システムのグループは、個々の最終システム又は最終システムの他のグループを含むものとして特定されてもよい。最終的に、通信リンクを経て、セキュリティが適用されるネットワークの外部の他のノードへ接続されるノードは、トポロジーデータベースに記入される。1つの実施形態において、シンタックスは、多層ファイアウォールのマネージメントドメイン以外の最終システムを表わす「外部」という名前の特殊な「仮想」ノードを与える。従って、トポロジーは、そのトポロジーにおける特定のノードが特殊なノード「外部」に接続されたかどうかを指示する。別の実施形態では、名前の付いた外部ノードが2つ以上存在することも考えられる。これは、多層ファイアウォールが、2つ以上の他の外部多層ファイアウォールと通信するためのポリシーを定義できるようにする。

又、セキュリティポリシー言語前部は、他の情報、例えば、ユーザ識別子、ユーザ識別子のグループ、行先へのアクセスがソースによって許される時間長さに

対する時間仕様、行先へのアクセスが許される時間間隔の仕様、等々を管理し、又はそれらを特定する前部として働くのが好ましい。

セキュリティポリシー言語それ自体は、ネットワーク内の最終システム間に許されたアクティビティを特定するセキュリティポリシーステートメントのセットを書き込むのに使用される。例示的なルールベース及びシンタックスは、次の通りである。

ソース	行先	アクセティ ビティ	ポリシー ステートメント	実施場所
ホスト1	ホスト2	FTP	「ジョン・ドウ」と 「ジェーン・ディア」 の従業員に対し月曜 -金曜の午前5時から 午後7時まで許可	行先
ホスト3	ホスト グループ 1	テルネット	不許可	行先
ホスト グループ 1	ホスト グループ 2	莫の音声	月曜-金曜の午前5 時から午後8時まで 許可	両方
ホスト グループ 2	ホスト1	HTTP	許可; オートデット	行先
外部	ホスト又 はホスト グループ	HTTP	許可	ソース
ホスト 又はホ ストグ ループ	外部	FTP	許可	ソース

トポロジー情報データベース

トポロジー情報データベースは、ノード及びそれらが互いに相互接続されたか
に関する情報を含む。ノードに特有の情報は、1つの例では、そのネットワーク
アドレス（1つ又は複数）と、そのMACアドレス（1つ又は複数）と、その許
された関連ユーザ識別子と、そのポート又はソケット番号と、セキュリティポリ
シーを実施する信頼があるかどうかと、実施できるのはどんな形式の実施ルール

かと、ノードにおけるセキュリティ構造のフォーマットと、ネットワークにおけ
るノード間の相互接続を含む。

ノードがいかに接続されるかの情報は、各ノード又はノードネットワークイン
ターフェイスの識別子と、どのノードがどのノードインターフェイスを経て他の
どのノードに直接接続されるかを特定するグラフ情報を含む。又、この情報は
、「外部」ノード、或いは外部接続を指示する別のファイアウォールシステム又は
別のデータ構造体に接続されたノードも含む。1つの拡張において、情報は、物

理的ノード内の個々のプロセスを識別する。

トポロジーデータベースは、一例において、単一のデータベースマネジメン
トシステムによって管理されるか、或いは個々のノード又はノードの集合におい
てデータベース前部システムにより管理される複数のデータベースから構成され
る。多数のデータベースにおけるデータは、例えば、RMON及びdRMONデ
ータと、最終システム及びネットワークデバイスにより管理されるセキュリティ
情報と、ネットワークを通して分散されたネットワークワークマネジメントシステ
ムにより得られる接続情報を含む。

セキュリティポリシーマネジメント後端

セキュリティポリシーマネジメント後端は、セキュリティポリシー前部コン
フィギュレーションインターフェイス及びトポロジーデータベースからの情報を
使用して、セキュリティポリシーステートメントにより特定されたセキュリティ
ポリシーを形成、記憶、更新、分配及び実施する。後端は、スタンドアローンマ
ネジメントシステム、永続的記憶システム及びノードにおけるエレメントより
成る。セキュリティポリシーマネジメント後端は、トポロジーデータベースに
おける情報のコンテックスにおいてセキュリティポリシーステートメントで特定
されたルールを变换し、そしてノード特有のセキュリティポリシーコンフィギュ
レーションデータを構成し、それが選択したネットワークノードへ分配する。セ
キュリティポリシーマネジメント後端は、セキュリティポリシーステートメン
トを、特定のノードで実施できるコンフィギュレーションデータのセットにいか
に区画化するかを判断し、そしてセキュリティポリシーステートメントのルール
を、その選択されたノードで実施できるノード特有のコンフィギュレーションデ

ータへと変換する。

ノード特有のセキュリティポリシーコンフィギュレーションデータは、ノード
のフィルタリングエンジンを実動するフィルタリングルールのような静的なデー
タを含むか、又はジャバ、ソース又はバイトコードのような動的なデータリンク
プログラムや、TCL、ピアル、Cシェルスクリプトのようなスクリプト言語
で表わされたプログラムを含む。特定のノードで実施されるセキュリティポリシ

ーステートメントを表すコンフィギュレーションデータのフォーマットは、特定のノード及びそのセキュリティポリシー実施エージェンツに基づく。

1つの別の形態において、セキュリティポリシーマネージャメント後端は、セキュリティポリシーステートメントが上記のシンタックスに基づいて表わされると仮定すれば、セキュリティポリシーステートメント及びプロパティデータベース情報を分析して、次のプロセスに基づきデバイス特有のセキュリティポリシーコンフィギュレーションデータを駆動する。

1. ノードは、2つの分類に分けられる。1) ポリシーを実施できないか又は実施する信頼性がないためにポリシーを実施することのできない受動的ノード、及び2) ポリシーを実施することのできる能動的ノード。

2. 各能動的ノードごとに、それに直結されるか、又は受動的ノードから他の受動的ノードを経て能動的ノードへ至る経路が存在するところの全ての受動的ノードのリストを形成する。このリストにおける各受動的ノードは、能動的ノードの関連ノードと称される。

3. 各セキュリティポリシールールに対して、ソースノードのセットを形成し(即ちリストが個々のノードのみを含むまでソースセットにおけるノードの全グループを繰り返し拡張することにより)、そして行先ノードのセットを決定する(ソースセットにおけるノードではなく行先セットにおけるノードを使用すること以外は同じ分解アルゴリズムを使用して)。

4. 各セキュリティポリシールールに対して、次の計算を実行する。ソースノードセットにおける各受動的ノードごとに、そこから、能動的ノードを横断しない行先ノードセットの受動的ノードへ至る経路が存在するかどうか決定する。もしそうであれば、ルールを実施できないことを通知する。

5. ルールが、ソースにおいて実施すべきであることを特定する場合には、

- ソースノードセットにおいて関連ノードを伴う能動的ノードのセットを決定する。
- これら能動的ノードの各々に対し、ルールで特定されたセキュリティポリシーステートメントを、ノードが実施できるセキュリティポリシー

ンフィギュレーションデータ、即ちそれ自身のセキュリティポリシーシーケンスのルールへと変換する。

- ノード特有の通信チャネルを使用してノードにおいてこれらルールを確立する。

6. ルールが、行先ノードセットにおいて実施すべきであることを特定する場合には、

- 行先ノードセットにおける関連ノードを使用する以外は、上記5の場合と同じことを行う。

7. ルールが、ソースノードセット及び行先ノードセットの両方において実施すべきことを特定する場合には、

- 上記5及び6の両方を行う。

上述したルールに基づくセキュリティポリシーの実施は、図2及び3を参照して良く理解することができよう。図2は、本発明によるセキュリティポリシーが多数の層において実施されるネットワークの要素を詳細に列示する。図3は、分散型多層ファイアウォールの実施を示す全体的なフローチャートである。

図2から明らかなように、代表的なネットワークは、種々様々なネットワークデバイス及び最終システムを備えている。従って、図2は、ノードのセットを含むネットワークを示し、ノードセットにおけるノードは、多数のプロトコル層にセキュリティ機能を与える。ネットワークは、汎用のワイドエリアネットワークWANファシリティ100を備えている。ワイドエリアネットワーク100は、第1のブライベートネットワーク101及び第2のブライベートネットワーク102に接続される。第1のブライベートネットワーク101の要素は詳細に示されているが、第2のブライベートネットワーク102は雲の形で示されている。又、ワイドエリアネットワークファシリティ100は、スタンダードアローンのル

タ型の最終システム103と、公衆交換電話ネットワーク(PSTN)105に接続されたラインサバ104と、これもPSTN105に接続されたアクセスサバ106とに接続される。図2に示すように、WANファシリティ100は、サイトルータ107、パケットサバ108及び別のサイトルータ109を経

てブライベートネットワーク101に接続される。

PSTN105は、モデム110を経てスタンダードアロンのダイヤルアップ最終システム111に接続される。又、PSTN105は、リモートアクセスルータ112に接続される。リモートアクセスルータ112は、最終システム113及び114に接続される。又、リモートアクセスルータ112は、ターミナルサーバ115に接続される。これは、次いで、最終システム116及び117に接続される。

第1のブライベートネットワーク101において、パケットサーバ108は、この例では中継器又はスイッチの機能を与えるハブ120に接続される。ハブは、次いで、サイトルータ107及びサイトルータ109に接続される。サイトルータ107、109の各々は、ワイドエリアネットワークアシリティ100にも接続される。サイトルータ107は、アクセスサーバ121に接続され、これは、PSTN105に接続される。又、サイトルータ107は、スイッチ122及びスイッチ123を含むスイッチセットに接続される。サイトルータ109は、スイッチ124に接続される。スイッチ124は、中継器125で表わされた中継器セットに接続される。中継器125は、図1のノード11に対応するセキュリティポリシーマネジメントリソースを含む最終ステーション126に接続される。

又、ブライベートネットワーク101は、スイッチ122及び123に接続された要素で表わされた多数の他のデバイスも含む。スイッチ122は、中継器130及び最終システム131のネットワークインターフェイスカードNICへの接続を含む構成で示されている。中継器130は、ネットワークインターフェイスカードを含む最終システム132を備えた最終システムセットにも接続される。

スイッチ123は、中継器133に接続され、これは、次いで、最終システム134を含む多数の最終システムに接続される。スイッチ123は、図中盤の形

で一般的に示されたスイッチネットワーク140に接続される。スイッチネットワーク140は、スイッチ141に接続される。スイッチ141は、中継器14

2に接続され、これは、次いで、ネットワークインターフェイスカードNICを含む最終システム143に接続される。

図2において、セキュリティポリシーマネジメントが配置されたノードは、水平のバーでコード化される。従って、図の左上の隅から始めて、モデム110、リモートアクセスルータ112、ターミナルサーバ115、アクセスサーバ106、ラインサーバ104、パケットサーバ108、サイトルータ107、サイトルータ109、スイッチ122、スイッチ123、中継器133、及び最終システム131、132のネットワークインターフェイスカードは、全て、セキュリティポリシーマネジメントを含む。ポリシーマネジメントステーション126は、上述したコンプライエンスインテンション、ポリシー、ポリシーデータベース、及びコンプライエンスインテンションドライバ後端を形成するリソースを備えている。

本発明に基づいてセキュリティポリシーマネジメントを実施できる典型的なネットワークにおけるデバイスの概要を以下に説明する。次いで、図3-6を参照して、本発明のプロセス全体を説明する。

ネットワークインターフェイスカード及びモデム

ノードセットにおける最も基本的な製品は、ネットワークインターフェイスカード(NIC)及びモデムである。NICは、内部I/Oバスを経て最終システムに取り付けられて、イーサネット、高速イーサネット、ギガビットイーサネット、トークンリング、FDDI及びATMのようなローカルエリアネットワークへの最終システムアクセスを与えるI/Oデバイスである。ATMの場合には、あるNICは、ATMのワイドエリアネットワークにアクセスすることができる。

モデムは、シリアル又はパラレルインターフェイスを経て最終システムに取り付けられる外部装置である。一般に、それらは、最終システムがPSTN又は非交換式の地上ラインを使用してデータを移動できるようにする。

従来、NIC及びモデムは、特徴ではなくて性能に対して最適化された簡単な装置である。

おそく、広範囲を受け入れを得るための第1のNICセキュリティ特徴は、NICブートROMである。ネットワークサーバからディスクなしでブートできるように最初に意図されたブートROMは、信頼性のあるブートコードの実行を保証するという関心のあるセキュリティ副作用を有する。ある支援ソフトウェアと共にこれを使用して、信頼性のあるコードを最終システムへロードし、このシステムがNICを確実に動作するよう構成する。

セキュリティの実施と共に益々普及した特徴は、フィルタリングである。フィルタリングの使用は、多数の目的により動機付けされる。LANレベルにおいてフィルタリングを使用し、フレームの無制限な送信から生じるリソース欠乏の問題からNIC及びハブが保護される。この形式のフィルタリングを与えるために開発された構造は、VLANとして知られている。層2より上で動作するより一般的な機構は、ルータを横切ってフィルタリングを行えるようにする。これらの機構は、VNETとして一般に知られている。

フィルタリングをセキュリティの目的に使用することは、NIC、スイッチ、中継器、ルータ及びリモートアクセス装置で行うことができる。NIC内でのフィルタリングは、それが送信するソースMACアドレスが有効であることを保証すると共に、それが受信するソースアドレスが信頼性のある最終システムからのものであることを保証するようために使用できる。しかしながら、NICフィルタリングは、他の等しく有効な目的にも使用でき、例えば、ハブからVLANの実行処理の負荷を除去し、浸透した多層ファイアウォールを実施し、そして高レベルセキュリティプロトコルに対するハードウェアサポートを与えるのに使用できる。

NIC及びモデムにとって独特の1つの保護通信特徴は、ある物理的な通信チャネルによって与えられる高レベルの流出セキュリティである。特に、光ファイバラインの使用は、侵入者による受動的な盗聴のおそれを低減する。

更に、多くの顧客は、彼等の内部ネットワークが、通信ポート及び最終システムへの物理的なアクセスを得ようとする侵入者に対して益々抵抗力的ない状態になりつつある。例えば、慎重さを要する資産的情報を保持する会社のイントラネットは、広い地域にわたって延びていて、遠隔のエンジニアリング及びセールス

オフィスがそれらに接続されている。これらの遠隔オフィスは、典型的な会社の構内に見られる同じレベルの物理的セキュリティを与えていない。

NIC及びモデムは、両方ともネットワークアクセス制御をサポートする特徴を与えることができる。モデムは、出ダイヤルシーケンスを実行する前に、ユーザがパスワードを与え、トークンカードを使用し、又はさもなければ、接続を開始することが許されたという証換を示すことを必要とする。又、モデムは、許可された電話番号からの接続だけを許すアクセスサーバにおいてコールドバック機能をサポートすることもできる。

セキュリティポリシーの後端は、例えば、更新されたNICブートコードを関連ネットワークサーバに記憶し、そしてNICに再ブートするよう通知することにより、NICにセキュリティルールを確立する。モデムにおいては、ドライバコードが更新されるか、又はモデムマネージメントコードとの通信により新たな値がコンフィギュレーションレジスタに書き込まれる。

中継器

ハブは、他の最終システムにフレームを送信しそしてプロトコルハイアラキーの層2に接続を与えるためにNICが接続されるスタースターネットワーク装置である。ハブを相互接続して相互接続ツリーを形成することによりハイアラキーネットワークを構築することができそしてそのようにするのが一般的である。

中継器は、それが受信したフレームをそれらの全てのライン（フレームが到着したラインを除いて）に放送するハブである。中継器は、低廉な相互接続組織を構築するのに有用である。しかしながら、相互接続された中継器の数が増加するにつれて、接続された最終システム間の干渉も増加する。それ故、中継器を使用して直接接続できる最終システムの数には限度がある。

中継器は、一般にコストを減少するために特徴を最小限に抑える基本的な放送デバイスである。しかしながら、それらにおいてセキュリティ特徴が実施されている。

層2における保護通信は、本来セキュリティに問題があるが、中継器によって少なくとも部分的に対処することができる。とりわけ、ある中継器は、フレームがアドレスされないセグメントにわたって放送されたフレーム内のデータを歪曲

する。これは、これらセグメントに取り付けられた探知機がこれらフレーム内のデータを見ることができないよう確保すると共に、衝突検出アルゴリズムが適切に働き続けるよう保証する。

高周中継器は、IEEE 802.10規格で定義されたような精巧な保護通信機構又はあまり複雑でない他の機構を実施することができる。このような機構は、フレームに保持されるデータを保護するために暗号化技術を使用する。このような保護は、浸透した多層ファイアウォール及びネットワークアクセス制御機構のようなシステムセキュリティ特徴を実施しそして最終システムデータの保護を与えるのに有用である。

従って、セキュリティポリシシー後端は、隣接マネージメントノード又はマネージメントリソースを中継器自身において更新することにより中継器にコンフィギュレーションデータを確立する。

スイッチ

スイッチは、フレームのソース及び先行アドレス（並びにおそらくは他の情報）を検査して、それらのラインのどれを使用して受信フレームを転送すべきか決定するハブである。中継器に属するスイッチの利点は、行先への経路上にあるラインのみを経てフレームを送信することにより最終システムへのトラフィックを減少することである。放送されたフレームの場合には、スイッチは、スイッチ内に保持されたポリシシー情報に基づきあるラインを経てそれらの中継しないように決定することができる。

ATM、イーサネット、高速イーサネット及びトークンリングスイッチを含む種々の能力及びコストのスイッチが製造される。ATMスイッチは、他のRAN形式に対して作られたスイッチより著しく複雑である。特に、ATMスイッチが相互接続されるときには、スイッチが最終システム間に確立した仮想回路を経てフレームを移動する。これは、最終システムからスイッチへ及びスイッチ間での制御情報の移動を必要とする。この形式のトラフィックは、他のアクセス技術のスイッチでは必要とされない。

又、中継器により実施される全ての機能は、スイッチでも実施できる（前記の説明を参照）。加えて、スイッチは、種々のフィルタリング機能を実行するのに

適した場所である。あるスイッチは、VLANサポートの形態でこれを行いうることができる。セキュリティを与えるのに加えて、VLANは、VLANメンバーのセグメントを経てフレームが放送されるのを阻止することによりスイッチ/中継器通信組織に流れるトラフィックの量を減少する。

フィルタリング機構は、従来、フィルタリングが適用されるフレームの種々の特性に基づいて受け入れ判断を行う。しかしながら、フレームの制御及び/又はデータを交換するというフィルタリングのより精巧な使い方ががある。例えば、浸透した多層ファイアウォールを実施するには、フレームを別の保護フレーム内にカプセル化し、層2のセキュリティを実施することが必要となる。層2のトンネルは、ATMスイッチ（LANエミュレーション）と、LANトラフィック搬送ATMセル（CIF）とによって既に実施されている。セキュリティトンネルの概念は、トンネル媒体を通過するときにトンネルトラフィックを保護することによりこれらの機構を拡張する。変換フィルタリングの別の分類は、層2アドレス変換であり、これは、浸透したファイアウォールの実施に有用である。

スイッチは、RADIUS、TACACS+及びネットワークエANDSのような認証、許可及びオーディット（AAA）サーバとの代理対話のようなヘッドエンドトワークアクセス制御機能を入れるための本来の場所である。スイッチは、中継器に関連して、ポートの切断及び再接続を監視し、これらをネットワークマネージメントアプリケーションに報告することができる。

又、スイッチは、セキュリティ支援特徴を入れるための便利な場所でもある。例えば、スイッチは、信頼のあるサーバのみがポート係を最終システムへ供給するよう確保するためにシステム認証プロトコルを実施することができる。スイッチは、承認ハイアラキーの最上位の公開キーを含む公開キー暗号化に使用されるトップレベル承認のようなあるセキュリティインフラストラクチャー情報を保持しそして分配することができる。

セキュリティポリシシー後端は、スイッチにおいて実施されるSNMPのようなマネージメント通信チャンネルを使用するか、又はアプリケーション層のピアピア通信プロトコルを使用してスイッチのセキュリティ構造を更新する。

ルータ

ルータは、それらのインターフェース間でパケットを移動し、これらパケットをソースと行先との間で進行させるための装置である。ルート指定の判断は、通常、パケットのソース及び行先ネットワーク層アドレス、及び他の情報（例えば、パケットのサービスオリティ、セキュリティオブションデータ及びホップカウンタ）に基づく。ルータは、次のことを含む多数の特性によりスイッチから区別される。即ち、1) ルータは、異なるアクセス媒体に接続されたインターフェース間でデータを移動し、2) 層2制御情報に基づくのではなく、層3パケットに保持された情報に基づいてルート指定を行い、そして3) 通常フレームを全てのインターフェースに放送しない。

しかしながら、ネットワーク業界における最近の傾向は、スイッチング及びルート指定を同じネットワークデバイスに一体化することである。多数のネットワーク会社は、異なるアクセス媒体フレームフォーマット間を切り換えるスイッチを製造し、従って、これらスイッチは、異なるアクセス技術に接続されたインターフェース間でデータを移動することができる。更に、IPマルチキャストのようない層3放送プロトコルが益々普及してきている。その結果、ルータは、現在、スイッチに非常に類似した放送機能を遂行する。従って、ルータとスイッチとの間に残された1つの重要な区別は、その機能を遂行するためにその情報を得る場所（プロトコル層）であると考えられる。

ルータとスイッチとの相違がこのように緩和したのに加えて、同じ装置でルート指定及びスイッチングの両方を遂行する多数の会社の製品が市場に出回っている。これについて特に注目すべきは、トラフィックパターンを追跡してIPパケットをルート指定するカリフォルニア州、サニーベールのイブシロンネットワーク社のルータ/スイッチである。特定のソースと行先との間のトラフィックが特定のスレッシッシュレベルに到達した場合には、ルータは、これらシステム間のパケットが比較的高価なIPルート指定プロセスをバイパスできるようにするカプトスルー層2接続を設定する。

ルータは、スイッチと同じ多数のセキュリティサービスを与えるが、プロトコルハイアラキーの層3ではこれを行なわない。層3の保護通信特徴を定義する

現在の活動は非常に多数ある。この活動は、IETFのIPSECワーキンググループを中心とする。IPSECは、公表されると共に開発中である1組の規格であって、最終システム及びルータがIPプロトコルに対して認証、完全性及び機密性サービスをいかに提供するかを規定する。このようなサービスを利用し、端一端保護と、中間ルータ間及びルータと最終システムとの間のトンネルの保護との両方を与えることができる。

又、ルータにより与えられる従来のフィルタリングサービスは、それらがファイアウォールの要素として働くことができるようにする。一般に、ファイアウォールは、ネットワーク層、搬送層及びアプリケーション層におけるパケットフィルタリングと、アプリケーション代行との2つの機能を遂行する。ルータは、一般に、最初のサービスしか与えない。しかしながら、ファイアウォール技術は、ルータ内に状態マシンを設けて、FTP制御トラフィック及びTCP接続開放パケットのような、それを通して転送されるパケットを追跡し、そしてこの保持された状態を使用して、フィルタリングプロセスを推し進めるといふ傾向である。この特徴は、パケットフィルタリングとアプリケーション代行との間の区別を不明瞭にする。

フィルタリングを適切に使用すると、顧客は、仮想ネットワーク(VNET)を実施することができる。VNETは、VLANの層3等効物である。それらは、層3の通信組織を経て移動されたトラフィックを個別のドメインに分離する。VNETに属さない最終システム及びLANセグメントには、そのトラフィックが見えない。

セキュリティポリシー後端とルータとの間の通信は、通常、アプリケーション層におけるピアピア通信である。もちろん、SNMPのようなマネージメントチャンネルを使用することができる。

リモートアクセス装置

リモートアクセス装置は、シリアルラインを経て送られる通信を、ルート指定されたトラフィックに変換する。更に、それらは、SPXキーブ・アライブ、ローカルノードエミュレーション、等のプロトコル代理処理をサポートする。

最終システムは、リモートアクセス装置(例えば、ターミナルサーバ)に直結

することもできるし、又は公衆交換電話ネットワーク(PSTN)を経て接続することもできる。より一般的な状態は、PSTNを通る接続であり、これは、アクセスサーバの使用を必要とする。

アクセスサーバ装置には2つの主たる使用目的がある。その第1は、プライベートイントラネットへのリモートアクセスを与えることである。この場合、アクセスサーバは、プライベートイントラネット内に配置され、スタンドアロンの最終システム及びリモートオフィスルータがPSTNを経てリモートアクセスできるようにする。リモートアクセス製品の第2の使用目的は、イントラネットサービスプロバイダー(ISP)ネットワーク内である。これらは、ISPの包含装置及びISPのイントラネット接続への加入者アクセスを与える。これら2つの使用目的は、若干異なるセキュリティ要求を有し、これについて以下に詳細に述べる。

リモートアクセス装置の2つの機能、即ちラインサービス及びパケット処理は、従来、同じシャシ内では実施されている。最近の顧客要求の変化、特に、公衆WANを使用してプライベート仮想ネットワークを実施するという要望に伴い、宛主は、これらの機能を、ラインサービス及びパケットサーバの2つの異なる製品に分離するようになった。顧客がこれらの製品を使用するときには、ラインサービスは、一方の側では、PSTNに接続され(又はおそらく最終システムに直接接続され)、そして他方の側では、WANに接続される。パケットサービスは、一方の側では、プライベートイントラネット又はISPファシリティに接続され、そして他方の側では、WANに接続される。各接続に対して、ラインサービスは、WANを通して(通常、暗号化技術を使用して)パケットサーバへ至る保護トンネルを形成する。ラインサービスへの接続は、スタンドアロンの最終システム又はリモートオフィスのルータ装置から到来する。

3つのリモートアクセスコンフィギュレーションが代表的である。

第1のWANアクセスは、公衆交換電話ネットワーク(PSTN)を経てそれらの内部リソース及びイントラネットへのアクセスを与えるためにISPにより使用される。アクセスサーバがPSTNに接続され、スタンドアロンの最終システムをもつクライアントに接続することができる。

第2は、リモートオフィス及びテレコミュニケーション装置にプライベートネットワークへのアクセスを与えるリモートオフィスアクセスコンフィギュレーションである。リモートアクセスルータは、PSTNを使用して、会社の構内又は他の組織のアクセスサーバに接続する。アクセスサーバは、次いで、リモートアクセスルータからプライベートイントラネットへネットワークトラフィックを転送する。

第3のコンフィギュレーション、即ちスプリットサーバアクセスは、ラインサービス及びパケットサーバ機能を個別の装置に分離する。ラインサービスは、シリアルラインマネージャメント及びデータ通信問題を取り扱い、一方、パケットサービスは、WANとプライベートイントラネットとの間のインターフェイスを取り扱う。

3つのコンフィギュレーションは、全て、ある種のネットワークアクセス制御を必要とする。WANアクセスの場合には、WANへのアクセスを与える前に、ユーザを認証しそして許可を与える。イントラネットアクセスに加えて、ローカルリソース(例えば、ローカルで管理される内容、eメールサービス、ウェブページ)へのアクセスも与えるISPも、ユーザがローカルリソースを使用できる前に、ユーザを認証しそして許可を与える。

リモートオフィスアクセスは、プライベートイントラネットを経てトラフィックを流せる前に、リモートオフィスを認証しそして許可を与えることを必要とする。ルータは、それ自体、ユーザを代表するものでないので、初期の接続セッション中に認証及び許可を与えねばならない。通常、これは、ユーザ(システムアドミニストレータの役割を果たす)がリモートアクセス装置に対して認証を行い、そしてこの装置が、認証チェックを遂行した後、プライベートイントラネットへの経路を開くことを必要とする。

スプリットサービスアクセスは、2つのネットワークアクセス制御判断を必要とする。その第1は、ラインサービスへのユーザアクセスを許し、そしてその第2は、パケットサービス、ひいては、プライベートイントラネットへのユーザアクセスを許すことである。二重ログインでユーザに負担をかけるのを回避するために、スプリットサービスアクセスに使用されるネットワーク機構は、パケットサー

バ又はブライベートイントラネットにより管理されたアクセス制御リソースを使用する。

して、ラインサーバへユーザを入れることができる。このような場合に、ラインサーバとパケットサーバ/ブライベートイントラネットは、同サーバへのユーザの入場を許可するように協働する。

リモートアクセスにとって重要な別のセキュリティサービスは、フィルタリングである。アクセスサーバ（一体的コンフィギュレーション又はスプリットコンフィギュレーションのいずれか）は、ファイアウォール機能を入れるための本来のポインタである。これは、2つの形式の一方をとることができる。最も簡単なものは、アクセスサーバ及びパケットサーバ（スプリットサービスアクセスの場合）において従来のファイアウォールパケットフィルタリングを行うことである。このようなフィルタリングルールは、装置を通過する全てのトラフィックに適用される。

より進歩したフィルタリング形式は、接続ごとのベースで適用されるフィルタリングルールを確立することである。即ち、ユーザがアクセスサーバを経て接続を確立するときに、そのユーザに特有の1組のフィルタリングルールがフィルタリングデータベースから引き出される。これらルールは、次いで、アクセスサーバにインストールされ、アクセスサーバは、その接続を経て進行するトラフィックのみにそれを適用する。

更に、保護通信は、リモートアクセスによって与えられる重要なサービスである。これは、2つの段階で行なわれる。ある状態においては、PSTNによって与えられる物理的なセキュリティでは、ユーザ/ブライベートイントラネットに適切な保証を与えるのに不十分である。このような場合に、モデム/リモートアクセスルータは、アクセス/ラインサーバとの通信を暗号技術で保護することができ。これは、シリアルラインにわたって実行される暗号プロトコルを必要とする。

より一般的なケースは、WANにわたる通信を保護する必要性から生じる。この状態においては、WANにわたりシリアルイントラフィックを移動するのに

必要なトンネルプロトコルが暗号化によって保護される。これは、トンネルプロトコル内でのセキュリティサポートの結果として生じるか、又はWANに使用されるネットワークプロトコルにより与えられるセキュリティ特徴を使用する結果

として生じる。後者の重要な例は、IPSECを使用して、IP WANの通信を保護し、これにより、仮想ブライベートネットワークを形成することである。

ネットワークマネージメント

実質上全てのネットワーク中間システム及びNICは、あるやり方で構成されるか、さもなければ、管理されねばならない。一般に、これは、簡単なネットワークマネージメントプロトコル(SNMP)を介して遂行され、これは、管理される各デバイスがリモートマネージメントソフトウェアにより制御されるエージェント機能を実施することを仮定する。通常、多数のエージェントが所与のマネージメントセッションにより管理される。

ネットワークデバイスは、通常、SNMPマネージャからの「ゲット・アンド・セット」要求に応答するSNMPエージェントを構成し、これは、サイトアドミニストレータが、デバイスごとではなく一体化されたシステムの観点からネットワーク装置を管理できるようにする。

あるネットワークマネージメントシステムの1つの重要な特性は、分散型リモート監視(dRMON)を与えることである。リモート監視は、LAN装置に接続された「ブローブ」から統計学的情報及びアラーム情報をネットワークマネージャに与える。しかしながら、LANセグメントの数が増加するにつれて、ブローブのリソースがその能力を越えてストレスを受け、不完全な情報がマネージメントステーションソフトウェアに送られることになる。この問題に対処するために、dRMONは、ブローブ機能の若干をNIC及びハブに分配し、これは、LANのサイズが成長するにつれてリモート監視機能を拡張できるようにする。

2つのネットワークマネージメントの問題は、重要なセキュリティの観点によって特徴付けされる。その第1は、ネットワークマネージメントセキュリティであり、即ちネットワークマネージメントサブシステムが破壊されないよう確保することである。重要なことは、アクセス制御機能であるVLAN、VNET又は

他のグループ形成をいかに確実に実施するかである。一般に、この活動の一部は中央で管理され、そして一部分がユーザの判断に委ねられる。従って、グループメンバーシップに対するアクセス制御は、2段階プロセスである。第1段階では、システムアドミニストレータは、グループを形成し、そしてユーザ又はシステムが参加するところのポリシーを確立する。第2段階では、ユーザは、グループに参加することを判断するか、又はシステムをグループに入れることを判断する。次いで、アクセス制御マシンは、グループに関連したポリシーデータを調査し、提案されたメンバーシップ要求が有効であるかどうか決定する。このアクセス制御判断の各段階は、秘保持持されねばならない。

他の形式のネットワークマネージメントセキュリティは、マネージメント情報ベース (MIB) へのアクセスを制御し、捕獲されたパケットのような重要なネットワークマネージメントデータの保護通信を行い、そしてネットワークマネージメントステーションへのアクセスを与えることである。

第2の重要なネットワークマネージメント問題は、セキュリティポリシーマネージメントである。上記の製品分類の各々は、正しく且つ機密保持されたオペレーションのためにポリシーデータを必要とするセキュリティ特徴を有する。NIC、スイッチ、ルータ及びリモートアクセス装置に対するフィルタリングルールが形成され、流布され、変更されそして検討される。中間サイズのネットワークの場合、これらのマネージメント機能は、フィルタリングデータに対して整合された制御がない限り、支持できないことになる。これは、確実且つ頑丈なセキュリティポリシーマネージメントシステムの使用を必要とする。保護通信、アクセス制御及びセキュリティ支援特徴に関連したセキュリティポリシーデータを管理するためには同様の要求が存在する。

フィルタリングパラメータ及び保護通信インフラストラクチャ情報のようなセキュリティポリシーデータを含むネットワークデバイスの数が増加するにつれて、そのセキュリティポリシーデータのコピレントで且つ整合されたマネージメントを与えることが益々重要となる。本発明によれば、アドミニストレータがセキュリティポリシーステートメントを入力できるようにするツールが設けられ、

このようなステートメントに対応するデータは、そのポリシーが実施されるネットワークに分散されたエージェントへと分布される。

ネットワーク内の種々のデバイスを制御するセキュリティポリシーデータは、種々のやり方で相互作用する。従って、コンフィギュレーションインタンフエイスは、ファイアウォール機能の多数の層を正しく管理するのに重要な異なるビュー

をアドミニストレータに与えるのが好ましい。例えば、ルータのフィルタリングデータは、ソースアドレス、TCPヘッダ情報、又はソース/先行アドレス対によって表示される。各ビューは、トラフィックが拒絶されるか、許可されるか又は変換されることに関する異なる情報をアドミニストレータに与える。

本発明のコンフィギュレーションドライバは、所望の振舞いを記述する高レベルのセキュリティポリシーデータを、個々のネットワークワークデバイスのセキュリティポリシーデータへとマッピングする。従って、高レベルの記述ポリシーステートメントが低レベルコンフィギュレーションデータのセットへとコンパイルされる。次いで、コンフィギュレーションデータは、例えば、簡単なネットワークマネージメントプロトコル (SNMP) 状のプロトコル、テルネット、トリビアルファイル転送プロトコル (TFTP)、又は他のデバイス特有のプロトコルを使用し、て適当なネットワークデバイスへと分配される。従って、ネットワークポロジデータベースは、コンフィギュレーションインタンフエイスに与えられるセキュリティポリシーステートメントに基づいてコンフィギュレーションデータをコンパイルしそして分配する目的で重要である。

簡単なネットワークの場合、システムアドミニストレータは、トポロジー情報を手で入力することができる。しかしながら、いかなるサイズのほとんどのネットワークについても、これは実用的なオブションでない。従って、必要なトポロジー情報を維持する従来のネットワークマネージメントツールは、本発明のコンフィギュレーションドライバに使用するようにトポロジーデータベース情報をコンパイルするのに使用できる。従来のネットワークマネージメントツールによって収集されたトポロジー情報と、本発明のセキュリティポリシー実施戦略との間に必要とされる相互作用のレベルは、実施される多層ファイアウォールの精巧

さに依存する。例えば、ネットワークポートプロジェに対する変更は、高レベルセキュリティポリシーデータと、要素デバイスに分配されるセキュリティポリシーデータとの間のマッピングを無効化することがある。精巧な多層ファイアウォールは、トポロジに変化が生じたときにネットワークマネジメントシステムからは、トポロジに変化が生じたときにネットワークマネジメントシステムから通知を受け取り、そしてそれに応じてポリシーデータ及びその要素デバイスを再構成するようにされる。

更に、セキュリティポリシーマネジメントツールは、侵入者がそれを使用し、ネットワークに侵入できないように保護される。これは、セキュリティポリシーコンフィギュレーションドライバート、ネットワークに分散されたエージェントとの間の保護通信を適当なアクセス制御手順に基づいて使用することを必要とする。

ネットワークの多数の要素がアクセス制御をサポートする。しかしながら、全ての要素が同じ種類のアクセス制御機構をサポートするのではない。共通のネットワークアクセス制御機能を、ネットワーク内のできるだけ多くのデバイスに与えるのが好ましい。例えば、広域網に配備された認証、許可及び会計サーバー、種々様々なネットワークデバイスを管理するように適応させることができる。更に、ネットワークのようなネットワークオペレーティングシステムは、あるAAサーバーを与える。

更に、ネットワークデバイスは、本発明に基づいてアクセス制御判断を分担することができる。簡単な例では、ラインサーバーへのアクセス制御は、スプリットアクセスコンフィギュレーションにおいてそれに関連したパケットサーバに委任することができる。これは、分散型リモートアクセスシステムの一貫した振舞いを確保するだけでなく、その複雑さを低減し、そして信頼性を高める。

従来のセキュリティ原理は、保護通信を端から端まで行なわねばならないとされている。しかしながら、動作条件によって時にはこれが最適でないこともある。例えば、資産的装置は、一端セキュリティプロトコルをサポートできない。これらのシステム間、又はそれらシステムと非資産的システムとの間の通信のセキュリティを確保するためには、資産的システムの代理として顧客ルータやスイッ

チャーのような非侵入の保護機構を必要とする。この解決策は、本来、端一端ではない。

高いセキュリティを必要とする共通の物理的環境においてある装置を共通配置することができる。このような環境では、境界の外側の装置とその内側の装置との間に端一端保護を与えることは有益でない。コストを最小限に抑えるために、保護を物理的セキュリティの境界で終わらせ、全ての内部システムの高価なハードウェア及びソフトウェアをサポートする必要性を排除することができる。

セキュリティプロトコルをサポートするには、高価な暗号化ハードウェアを使用することが必要となる。ある場合には、このハードウェアを全てのシステムに経路的に設置することができない。これは、データの最終的な行先より前のどこかで暗号化ハードウェアを実施するシステム又はデバイスでは保護通信経路を終わらせねばならないことを意味する。

これらの状態を受け入れるために、ソースと行先との間の経路の構成セグメントにおいて異なる手段により保護通信を行うことが必要である。幾つかのセグメントは、層3の保護通信を使用し、一方、他のセグメントは、層2の保護を使用する。各セグメントにより与えられる保護を、充分な端一端セキュリティを確保するように整合するには、これらのセグメントが互いに協調することが必要になる。本発明は、このような協調を管理できるツールを提供する。

図3は、本発明による多層ファイアウォールを実行するのに使用されるプロセスのフローチャートである。上述したように、図3に示すノードは、ネットワーク内の多数のプロトコルレベルで動作する種々様々なネットワークデバイス、最終システム、並びにこれらネットワークデバイス及び最終システムで実行される機能に対応する。

図3に示すように、第1段階は、ネットワークポートプロジェ及びセキュリティルールを決定する(ステップ300)。この情報は、図1のシステムにおいてコンフィギュレーションインタンクフェイス及びポートデーター配極装置によって与えられる。

次いで、ネットワーク内の全ての能動的ノード及び受動的ノードが識別される。

(ステップ301)。各能動的なノードに対し、能動的なノードを介在せずに能動的なノードに接続された受動的なノードが識別される(ステップ302)。これは、能動的ノードのセットを、コンフィギュレーションデータのコンパイルに使用されるべき関連する受動的ノードと共に定義する。例えば、図2を参照すれば、能動的ノードは、ポリシーを実施することのできるノードを含む。受動的ノードは、ポリシーの実施が与えられないか又は信頼されないノードを含む。従って、受動的ノードは、最終システム143、中継器142、スイッチ141、スイッチネットワーク140、スイッチ124、中継器125、及びネットワーク

内の他のデバイスを含む。

各セキュリティポリシールールに対し、最終ステーションのソース及び先行セッットが識別される(ステップ303)。ソース及び先行セッットは、各々、単一の最終ステーション又は最終ステーションのグループを含む。次いで、プロセスは、ルールを実施できるかどうか決定する(ステップ304)。上述したように、これは、例えば、ソースセッットの受動的ノードから先行セッットの受動的ノードへ至る経路であって、ルールを実施すべきプロトコル層において動作する能動的ノードを横断しない経路があるかどうか決定することを含む。ソース及び先行セッットにおいて受動的ノード間の接続が見つかった場合には、ルールを実施することができない。従って、ルールを実施できない場合には、セキュリティプロセスに通知され(ステップ305)。そしてアルゴリズムは、コンパイルされるべきルールがまだあるかどうか決定する(ステップ306)。コンパイルされるべきルールがそれ以上残されていない場合には、ステップ307で示すように、アルゴリズムは終了となる。更にルールがセキュリティポリシーに存在する場合には、アルゴリズムは、ステップ303へループして戻る。

ステップ304において、セッット内の識別された能動的ノードでルールを実施できることが決定された場合には、次いで、そのルールがソースで実施されるか、先行で実施されるか又はその両方で実施されるよう意図されたかどうか決定される。ルールがソースで実施されるべきであることを指定する場合には、ソースセッットのノードと先行セッットのノードとの間に介在する能動的ノードが識別され

、そしてルールは、ソースノードの1つがその関連セッットにあるところの能動的ノードのコンフィギュレーションデータに変換され、そしてこれらノードにおいて確立される(ステップ310)。

ルールを先行において実施するか又は先行及びソースの両方において実施すべき場合には、先行セッットのノードに関連した各能動的ノードに対し、ルールは、その能動的ノードのコンフィギュレーションデータに変換され、次いで、そのノードにおいて確立される(ステップ311)。

ステップ310及び311の少なくとも1つの後に、アルゴリズムは、変換されるべきルールがもつとあるかどうか決定する(ステップ312)。それ以上の

ルールがない場合には、アルゴリズムは終了となる(ステップ307)。変換されるべきルールがもつとある場合には、アルゴリズムは、ステップ303へループして戻り、プロセスを続ける。

ソース及び先行セッットが識別されると、先行セッットのノードに到達するために能動的ノードを横断する必要がある経路が受動的ノード間にあるかどうかを決定するプロセスは、WAN100に接続されたブライベートネットワーク102及びスタンドアローン最終システム103を考慮することによって理解することができ。これらネットワークセグメントにおけるノードは、ポリシーを実施できないか、又はポリシーを実施する信頼がない。従って、ブライベートネットワーク102及びスタンドアローンのルータ型最終システム103のノードが、特定のルールに対し、ソース及び先行ノードセッットに各々存在する場合には、そのルールをこれらノード間で実施することができない。しかしながら、ノード103及びブライベートネットワーク102の両方が、特定のルールに対してソースノードセッットに存在するが、ブライベートネットワーク101の全てのノードが、特定のルールに対して先行セッットに存在する場合には、おそらくルールを実施できることになる。というのは、ソースセッットと先行セッットとの間を通信するためには、全ての通信がルータ107、パケットサーバ108又はルータ109のいずれかを横断しなければならず、これらは全てポリシーを実施できるからである。

図4は、ある環境において多層ファイアウォールを改良することのできるプロ

セスを示す。例えば、図3のステップ303において、プロセスは、ソース及び行先セットのノード間の経路（1つ又は複数）において能動的ノードの「最小カット頂点セット」を識別するように分岐する（ステップ400）。カット頂点セットとは、除去された場合にソースセットと行先セットとを分離する能動的ノードのセットより成る。最小カット頂点セットとは、所与のソース及び行先セットに対して最小数のノードを有するセットである。従って、図2を参照すれば、例えば、ソースセットが最終ステーション113、114、116及び117を含む、そして行先セットがスタンドアロンルータ型最終システム103である場合に、能動的ノードの最小カット頂点セットは、リモートアクセスルータ112より成る。

リモートアクセスルータ112を通る各経路には、ソースセットに関連した能動的ノード（112及び115）及び行先セットに関連した能動的ノード（104及び106）に見られるものより少数の能動的ノードしかないもので、ある場合には、最小カット頂点セットの能動的ノードでのセキュリティポリシーの実施を、セキュリティポリシーをソース及び行先セットの全ての能動的ノードへ分配して実施するものよりも効率的に行うことができる。従って、アルゴリズムは、次いで、最小カット頂点セットの能動的ノードにおいてルールを効率的に実施できるかどうかが決定する（ステップ401）。もしそうでなければ、アルゴリズムは、ステップ402で示されたように、図3のステップ304へ復帰する。最小カット頂点セットの能動的ノードにおいてルールを実施できる場合には、ルールが、カット頂点セットにおける能動的ノードのコンフィギュレーションデータに交換され、そしてこのようなノードにおいて確立される（ステップ403）。ステップ403の後に、プロセスは、図3のアルゴリズムのステップ304へ復帰する。

図5は、ネットワークを通して分散されたセキュリティポリシーエージェントにおいてコンフィギュレーションデータを確立するためのプロセスを示す。

より詳細には、ノードにルールを確立するプロセスは、コンフィギュレーションデータをノードに転送し、それを永続的記憶装置に記憶し、そして新たなルールを実行できるようにデータが更新されたことをノードに確認させることを含む

。しかしながら、ネットワークに分散された全てのセキュリティエージェントが、ディスクドライブや不揮発性フラッシュメモリデバイスのような永続的記憶装置に直接接続されるのではない。例えば、中継器133は、永続的記憶能力をもたないことが考えられる。しかしながら、スイッチ123、又は更に好ましくは、ポリシーマネージャメントステーションの一部分を形成する最終ステーション126は、ディスクドライブ又は他の永続的記憶能力を有する。この状態において、コンフィギュレーションデータをスイッチ123、最終ステーション126又はネットワーク内の別のサーバに与え、そしてコンフィギュレーションデータが更新されたことを中継器133に通知することができる。中継器133に関連したマネージャメントエージェントは、次いで、再ブートの際に、又はコンフィギュレーションデータを更新する必要がある他のプロセスの間に、スイッチ123又は

最終ステーション126からコンフィギュレーションデータを検索する。

従って、ノードにルールを確立するプロセスが図5に示され、ステップ500で始まる。このプロセスは、先ず、コンフィギュレーションデータの対象ノードが永続的なコンフィギュレーション記憶装置を含むかどうか決定する（ステップ501）。もしそうであれば、コンフィギュレーションデータがそのノードの永続的な記憶装置へ送られる（ステップ502）。ノードが永続的な記憶装置を含まない場合には、コンフィギュレーションデータの対象ノードによってアクセスできるノードの永続的な記憶装置にコンフィギュレーションデータが送られる（ステップ503）。次いで、コンフィギュレーションデータの対象であるノードに変化を示す信号が送られる（ステップ504）。変化が生じたという信号を受信した後に、ノードは、更新されたコンフィギュレーションデータを検索する（ステップ505）。ステップ502又はステップ505のいずれかによってコンフィギュレーションデータがノードに送られた後に、ノードは、それが受け取ったコンフィギュレーションデータに基づいて新たなルールを実行する（ステップ506）。

従って、セキュリティポリシーマネージャメントコンフィギュレーションドライ

バーは、これらルールのコンフィギュレーションデータをノードに通信することによりノードにルールを確立する。例えば、ノードが永続的な記憶装置を有する場合には、セキュリティポリシーマネージャメントコンフィギュレーションドライバは、テルネット又はトリビアル・ファイル搬送プロトコル(TFTP)のよいうな標準的なプロトコルを使用してルールをノードへ直接通信するか、又は多層ファイアウォールの一部分としてこの目的のために特に指定されたプロトコルを使用する。ノードが永続的な記憶装置をもたない場合には、セキュリティポリシーマネージャメントコンフィギュレーションドライバは、ノードによってアクセスできる永続的な記憶装置にルールを通信し、次いで、例えば、SNMP又は別のプロトコルを用いてノードに信号を送り、セキュリティポリシールールが更新されたことをノードに通知する。次いで、ノードは、新たなセキュリティポリシールールを永続的な記憶装置から検索することができる。更に、別のシステムにおけるセキュリティポリシーマネージャメントコンフィギュレーションドライバは分散型データベース解決策を用いてノードポリシーを更新する。例えば、セキュリティポリシーマネージャメントコンフィギュレーションドライバは、ノードがキャッシュコピーを有するところのファイル又はデータベースエントリにデータを書き込むことができる。この分散型データベースキャッシュコヒレンシアリズムは、次いで、そのキャッシュコピーがもはや有効でないことをノードに通知し、マスターコピーを再読み取りするよう動機付ける。

各能動的ノードにおいてルールを実施すべきかどうか決定するための上記アルゴリズムは、本発明の多層ファイアウォールシステムの能力を例示するものに過ぎない。他のアルゴリズムも考えられる。例えば、セキュリティポリシーステートメントは、特定のセキュリティポリシールールにおいて、異なる能動的ノードで実施される部分に分解することができる。これは、ソースセットのノードと先行セットのノードとの間の経路を分析し、この経路における各能動的ノードにサポートされる意味を決定し、そしてこのセットの能動的ノードにおいてポリシールールの種々のセグメント又はポリシールールの冗長バージョンを実施することが必要とする。これらの能動的ノードにおいてセキュリティポリシールールを順

次に適用すると、ソース、行先、又はカット頂点セットの能動的ノードにおいて実施することのできないポリシーを実施できるので、分散形態でルールを実施するこの解決策は、より効率的なファイアウォールを与えることができる。更に、ノードの順次経路に沿ってポリシーの実施を分解することにより、ソース、行先又はカット頂点セットの能動的ノードにおける実施では考えられない効率を与えることができる。

図6及び7(図2と同様)を参照して説明する2つの例は、多層ファイアウォールが実際にいかに作用するかを示す。図6及び7において、ホストグループ1(600)は、中継器(604及び605)及びスイッチ(606及び607)を経て2つのサイトルータ608の一方に接続された多数の最終システム601、602、603...より成る。ホストグループ2(610)は、中継器613及びスイッチ614を経て他のサイトルータ615に接続された2つの最終システム(611及び612)より成る。2つのサイトルータは、スイッチ620を経て相互接続される。

両方の例において、多層ファイアウォールは、1つのポリシールールで構成される。

ソース	行先	アクティビティ	ポリシーステートメント	実施場所
ホストグ ループ2	ホストグ ループ1	FTP	許可	両方

このルールは、多層ファイアウォールポリシーマネージャメントステーション625においてセキュリティアドミニストレータによって入力される。

第1の例(図6)においては、2つのスイッチ606及び607は、中継器604及び605を経てホストグループ1(600)に接続され、ファイアウォールの実施を行うことができ、そしてスイッチ614及び中継器613によりホストグループ2(610)に接続されたサイトルータ615も、ファイアウォールの実施を行うことができる。

多層ファイアウォールポリシーマネージャメントステーション625は、多層フ

ファイアウォールポリシールールを2つのノード特有のポリシールールに分解し、その一方は、サイトルータ615に対するものであり、そしてその他方は、2つのスイッチ606及び607に対するものである(両スイッチは、同じデバイス特有のポリシールールを受け入れると仮定する)。「実施場所」の項は、「両方」を指定しているので、多層ファイアウォールポリシーマネージメントステーション625は、ノード特有のポリシールールを、TFTPのようなプロトコルを使用するサイトルータ615と、TFTPのようなプロトコル又は下位層SNMPを使用する2つのスイッチ606及び607との両方にダウンロードする。「実施場所」の項が「ソース」を指定する場合には、多層ファイアウォールポリシーマネージメントステーション625は、サイトルータ615に対するポリシールールのみをダウンロードする。「実施場所」の項が「行先」を指定する場合には、多層ファイアウォールポリシーマネージメントステーション625は、スイッチ606及び607に対するポリシールールのみをダウンロードする。

第2の例(図7)は、第1の例と同じネットワークポロジを有する。しかしながら、ポリシーの実施は、第1の例とは異なるやり方で行なわれる。特に、中継器604及び605を経てホストグループ1(600)の最終システムに接

続されたスイッチと、これらの最終システムにおけるNICとの両方は、ノード特有のポリシールールを実施することができる。加えて、中継器613を経てホストグループ2(610)に接続されたスイッチ614は、ノード特有のポリシールールを実施できるが、サイトルータ615は、実施できない。

多層ファイアウォールポリシーマネージメントステーション625は、多層ファイアウォールのポリシールールを2つのノード特有のポリシールールに分解し、その一方は、中継器を経てホストグループ2(610)に接続されたスイッチ614に対するものであり、そしてその他方は、ホストグループ1(600)に接続された2つのスイッチ606及び607に対するものである(この場合も、これらスイッチの両方が、同じデバイス特有のポリシールールを受け入れると仮定する)。「実施場所」の項は、「両方」を指定しているので、多層ファイアウォールポリシーマネージメントステーション625は、ノード特有のポリシールール

ルを、ホストグループ2(610)のスイッチ614と、ホストグループ1(600)の2つのスイッチ606及び607との両方にダウンロードする。「実施場所」の項が「ソース」を指定する場合には、多層ファイアウォールポリシーマネージメントステーション625は、適当なポリシールールをホストグループ2(610)のスイッチ614のみにダウンロードする。「実施場所」の項が「行先」を指定する場合には、多層ファイアウォールポリシーマネージメントステーション625は、適当なポリシールールをホストグループ1(600)のスイッチ606及び607のみにダウンロードする。

この例は、NICが多層ファイアウォールに参加する1つの方法も示している。ホストグループ1(600)に関連した各スイッチ606及び607は、そのノード特有のポリシールールを受け取ると、それが接続されたホストグループ1(600)の各最終システム601、602及び603へポリシールール情報を放送する。例えば、ホストグループ1(600)のスイッチ606及び607に対するノード特有のポリシールールは、次のようになる。

ソース	行先	アクティビティ	ポリシーステートメント
ホスト611	ホスト601	FTP	許可
ホスト612	ホスト601	FTP	許可

ホスト611	ホスト602	FTP	許可
ホスト612	ホスト602	FTP	許可
*	*	*	*
*	*	*	*
*	*	*	*

このテーブルにおいて、ホストグループ2(610)の各最終システム611及び612は、行先であるホストグループ1(600)の各ホストに対するソースとして特にリストされている。実際の場合には、ホストグループ2(610)及びホストグループ1(600)の最終システムに関連したサブネットアドレスをリストすることによりこれらルールをより効率的に表すことができる。

最終システム601のNICのような各NICは、これらのルールを受け取る

と、その最終システム（例えば、601）が行先ではないところのノード特有のポリシールールを全て破棄する。次いで、残りのルールを使用して、最終システム（例えば、601）に到着するパケットをフィルタする。この例では、ノード特有のポリシールールを実施するNICを伴う最終システム601、602及び603は、ホストグループ2（610）における最終システム611及び612からのFTP要求以外のトラフィックを受け取ることができない。

ホストグループ1（600）のスイッチ606及び607は、これらのルールを使用するが、ホストグループ1（600）の最終システム601、602及び603から到来するトラフィックに対してのみである。特に、それらは、ホストグループ2（610）の最終システム611及び612を行先とするFTP応答ではない全てのパケットをドロップする。これらのスイッチ606及び607は、それらが中継器604及び605を経て接続されない最終システムの行先アドレスを特定するノード特有のルールを破棄する。

この例において示される効果は、NICがインバウンドトラフィックに対して多層ファイアウォールポリシールールを実施する役割を果たし、一方、スイッチがアウトバウンドトラフィックに対してそれを実施する役割を果たすことである。この実施に対する役割を分割することにより、ホストグループ1（600）のスイッチ606及び607からある処理の負荷を取り去る。敵対するトラフィック

に対して最終システムを保護するようにNICに依存することによりこれが行われる。

両方の例において、多層ファイアウォールマネージメントステーション625は、デバイス特有のポリシールールをデバイスへ直接通信する。この解決策は、説明を簡略化するが、多層ファイアウォールマネージメントプロトコルに複雑さをもたらす。他の実施戦略も考えられ、望ましいものがある。例えば、ノード特有のポリシールールをデバイスに直接分配するのではなく、多層ファイアウォールマネージメントステーション625は、それらを永続的記憶装置に記憶し、そして新たなポリシーを検索するように各デバイスに通知することができる。第2

の例では、ホストグループ1（600）のスイッチ606及び607は、最終システム601、602及び603のNICにノード特有のポリシーを直接放送するのではなく、永続的な記憶装置から新たなポリシーを検索すべきであることを通知するメッセージをそれらに放送してもよい。

本発明の多層ファイアウォール機能は、1つの実施形態では、オブジェクトベースのマネージメントシステムとして実施され、そして他の実施形態では、分散型多層ファイアウォールの構成を与える目的で他のプログラミング技術で実施される。

本発明は、種々様々なネットワークデバイス及び最終システムより成るネットワークにおいて整合された多層型の浸透したファイアウォールを形成するフレームワークを提供する。このシステムは、セキュリティポリシールールを高レベルで指定するコンフィギュレーションインタンクウェアイスをベースとする管理し易い前段を与える。これらのルールは、次いで、ルールによって作用を受けるネットワーク内のノードに対する実際のコンフィギュレーションデータに分解される。このコンフィギュレーションデータは、次いで、ルールを実施するためにネットワークのノードにおいて確立される。ネットワークのトポロジー及びネットワークのノードで実行されるセキュリティ機能の形式に関する情報を使用して、このプロセスをルールごとに行うことにより、整合された浸透した多層ファイアウォールシステムが提供される。本発明によれば、ファイアウォールの種々の要素の役割分担が、好ましくは、グラフィックユーザーインターフェース及び高レベ

ルスクリプトのような使い易い特徴を実施する1つ以上のインテリジェントマネージメントシステムに集合される。

本発明の多層ファイアウォールは、無類の融通性をもつネットワークシステムのセキュリティインフラストラクチャを提供する。更に、種々様々なネットワークにおける多数のデバイスの複雑な管理を可能にするコヒレントな前段が提供される。

本発明の好ましい実施形態の以上の説明は、本発明を単に例示するもの過ぎない。本発明は、これに限定されるものではなく、請求の範囲に記載した本発明

の範囲内で多数の種々の変更がなされ得ることが当業者に明らかであろう。

【図1】

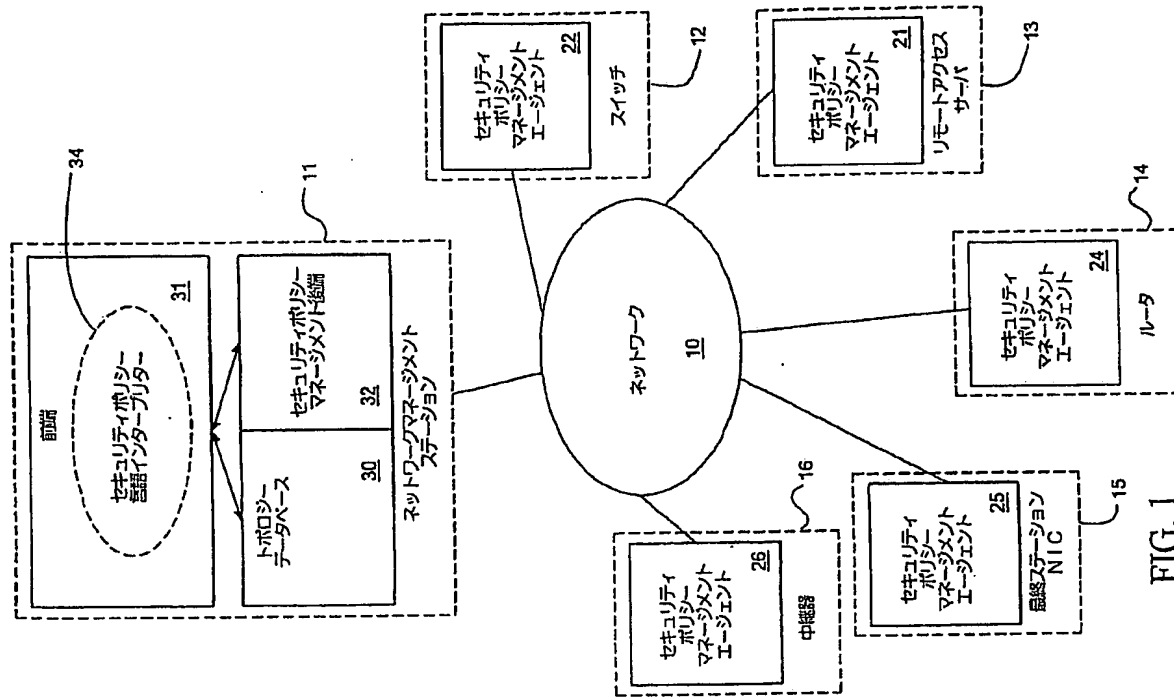


FIG. 1

【図2】

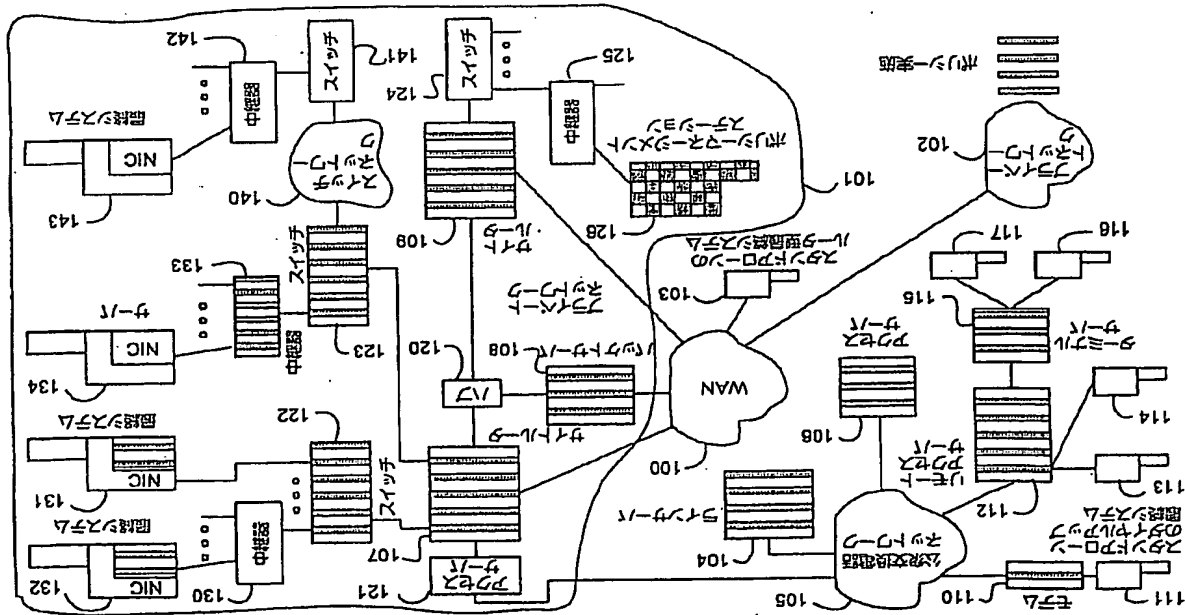


FIG. 2

【図3】

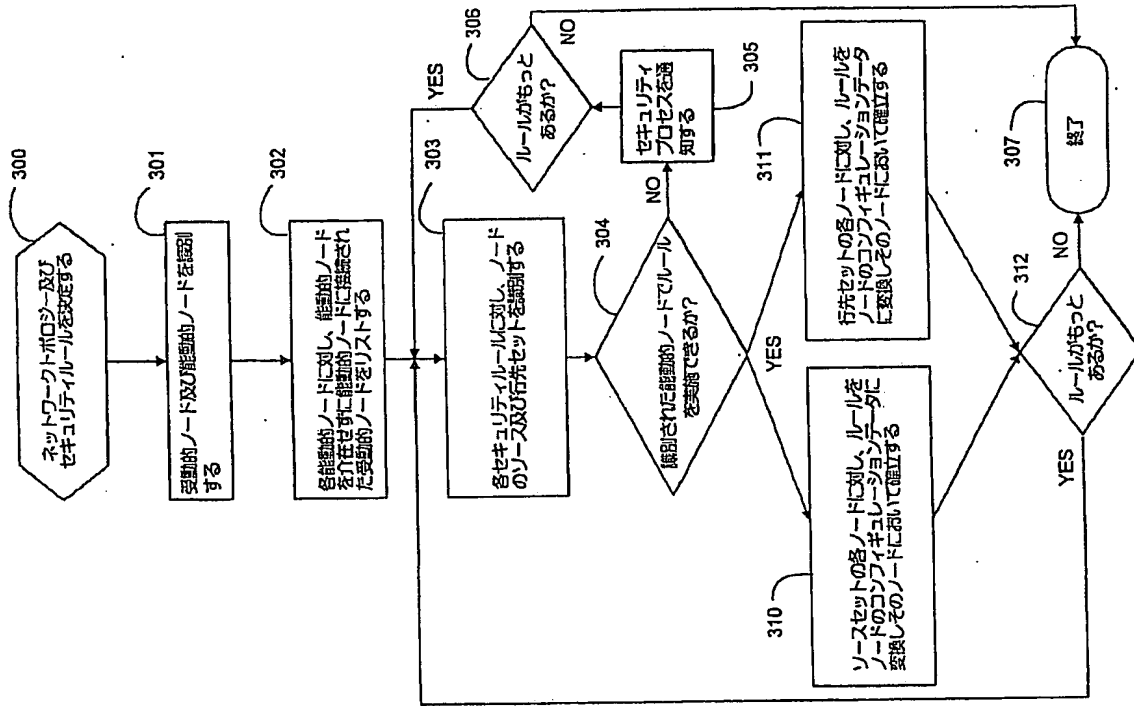


FIG. 3

【図4】

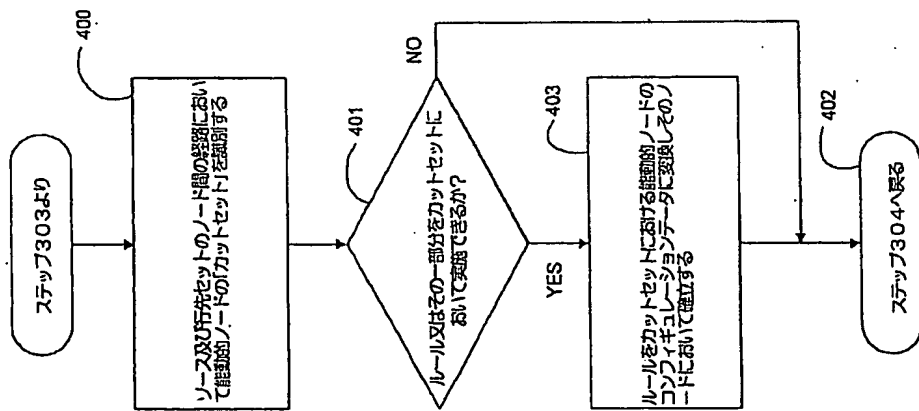


FIG. 4

【図5】

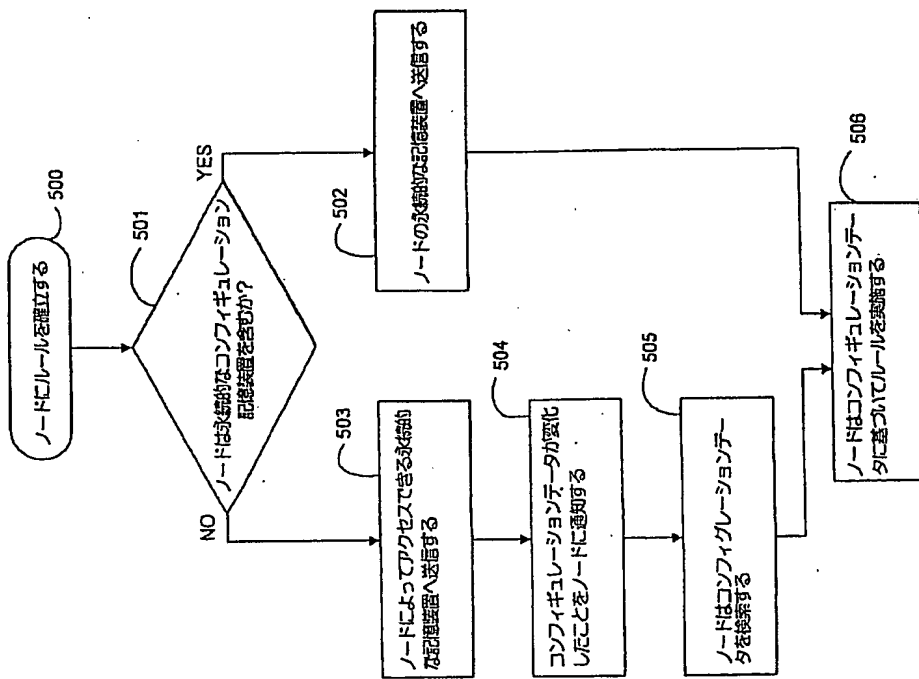


FIG. 5

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/0817

A. CLASSIFICATION OF SUBJECT MATTER

IPC(A) : G06F 11/00
US CL. : 391/107.01
According to International Patent Classification (IPC) or to both national classification and IPC

B. FIELDS SEARCHED

Minimum documentation searched (classification system followed by classification symbols)
U.S. : 391/107.01, 108.01, 165, 200.39, 200.53, 453, 310/071, 25

Documentation has related other than minimum documentation to the extent that such documents are included in the fields searched

Electronic data base consulted during the international search (name of data base and, where predictable, search terms used)
APR, INTERNET

C. DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevance to claim No.
Y	CHECK POINT SOFTWARE TECHNOLOGIES LTD. "Check Point Software Unveils Open Security Platform Strategy". http://www.checkpoint.com . 18 November 1996. See entire document.	1-15, 17, 21-22, 24-25, 43, 45-49 and 55-63
Y	SIMON et al. "Adage: An Architecture for Ambidextrous Authorization". OSF Research Institute. 2 December 1996. pp. 13-17.	1-15, 17, 21-22, 24-25, 43, 45-49 and 55-63
Y, P	US 5,740, 375 A (DUNNIE et al) 14 April 1998, col. 1, lines 22-34; col. 3, lines 12-32.	2-5, 9-14 and 55-58
A	US 4,881,263 A (HERBISON et al) 14 November 1989, col. 19, lines 8-42.	1-71

* Further documents are listed in the continuation of Box C. ☐ See patent family annex.

- * "A" documents published after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "B" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "C" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "D" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "E" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "F" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "G" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "H" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "I" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "J" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "K" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "L" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "M" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "N" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "O" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "P" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "Q" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "R" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "S" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "T" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "U" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "V" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "W" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "X" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "Y" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.
- * "Z" documents published on or after the international filing date or priority date and which are not cited in the international search report are not cited in the international search report.

Date of the search completion of the international search

19 AUGUST 1998

Date of mailing of the international search report

29 SEP 1998

Name and mailing address of the ISA/US
Consultation of Patent and Trademarks
Box PCT
Washington, D.C. 20541
Telephone No. (703) 305-3239
Facsimile No. (703) 305-9771

Authorized officer
ROBERT BEAUSOLEIL
Telephone No. (703) 305-9771

Form PCT/ISA/210 (revised January 1997)*

INTERNATIONAL SEARCH REPORT

International application No.
PCT/US98/0817

C (Continuation). DOCUMENTS CONSIDERED TO BE RELEVANT

Category*	Citation of document, with indication, where appropriate, of the relevant passages	Relevance to claim No.
A	US 5,577,209 A (BOYLE et al) 19 November 1996, see entire document.	1-71
A	US 5,606,668 A (SHWED) 25 February 1997, see entire document.	1-71
A	BLAZE et al. "Decentralized Trust Management". IEEE Conference on Security and Privacy. May 1996. See entire document.	1-71
A	CHECK POINT SOFTWARE TECHNOLOGIES LTD. "Check Point Software Brings 'Write Once, Manage Everything' Functionality to Enterprise Security Management". http://www.checkpoint.com . 22 October 1997. See entire document.	1-71
A	CHECK POINT SOFTWARE TECHNOLOGIES LTD. "Open Security Manager Data Sheet". http://www.checkpoint.com . 1998. See entire document.	1-71

Form PCT/ISA/210 (continuation of second sheet (July 1997))*